REGULATION OF THE DIGITAL ECONOMY FOR PROTECTION AGAINST LARGE PLATFORMS

Por

ANDRÉS BOIX PALOP / ALBA SORIANO ARNANZ
Lecturers in Administrative Law
University of Valencia

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

This monographic issue of the Revista General de Derecho de los Sectores Regulados, published by Iustel, which is the eighth number of this journal, thus reflecting its full consolidation, is a great satisfaction for us. Firstly, because of the possibility of having compiled, selected and reviewed these works for publication in a journal such as this one, which is already well established and with a proven track record of quality, and which is leading academic reflection on the legal regime of sectors which are becoming increasingly important and in need of publications with the rigour and usefulness of this one. Secondly, because we believe that the final result of the compilation we have achieved is of enormous interest, shedding legal light on some of the most topical issues regarding the regulatory challenges posed by the growing emergence of digital platforms in more and more sectors of economic activity, in a position as intermediaries which, thanks to the technology they use and the efficiency gains they have generated, gives them enormous market power. Finally, because these works constitute part of the results of initiatives for the internationalisation of legal research that we have been trying to promote from various research groups at the University of Valencia, which, in our modest opinion, are beginning to bear excellent results. The papers presented in this issue have been selected from among the proposals that were finally accepted for presentation at the Summer School of the Jean Monnet European Network on Sharing Economy and Inequalities Across Europe (SHINE) held in July 2021 at the Universitat de València on the study of issues such as the digital economy, technological innovation and its effects on inequalities (Digital Economy, Technology and Inequalities).

We have entitled the monograph "The regulation of the digital economy for protection against large platforms" because we believe that most of the reflections we have selected

are threaded around this idea, as well as the added value that, in our opinion, they can provide from the study of these conflicts.

The monograph opens with studies on the regulation of these markets in order to contain the risks that the growing control of the large platforms may pose to them, beginning with the work of one of us (Andrés Boix Palop, Universitat de València: Digital Platform Competition Regulatory Challenges") on the challenges that the peculiar position that digital platforms have achieved and some of the characteristics of the functioning of the digital economy pose when it comes to applying in a useful way the traditional competition guidelines that had been established by our competition authorities in recent years based on their analysis of anti-competitive dynamics in other types of markets. The conclusion is that some of these guidelines no longer serve to contain the effective competition problems, and also social problems, that can be generated by the new positions of dominance in the digital economy and that, consequently, some of these criteria need to be adapted.

Next, José Vida Fernández (Universidad Carlos III de Madrid) offers us "Una aproximación al régimen jurídico de los servicios digitales: estructura y sistemática del marco jurídico de los servicios prestados en línea", where he tries to expose in a synthetic, clear and complete way the structure of the legal framework referred to European (and Spanish) digital services, structuring it in an orderly and systematic way, where the legislator (or the concurrence of legislators) have been rather disorderly, in order to help us to determine the legal regime applicable to each of these services within the digital environment.

In a clearly complementary line, Carmen Rodilla Martí (Universitat de València) explains in her paper "Digital platform markets: between competition law and regulation" how the integration processes of these platforms and their growing market power require a combined use of Competition Law tools, but duly adapted and sharpened, together with the establishment of regulatory guidelines specifically designed to control these new hegemonic operators, with the added value of proposing some (and very interesting) specific solutions.

A third work, also more focused on the regulation of the activity of these platforms and the control of some of the pernicious effects that may arise for certain collective and individual interests, through the establishment of specific legal rules that seek to maximise the benefits of their activity and contain some of the possible abuses that may occur in the digital economy, is the study presented by Michael Fehling and Nico Schröter (Bucerius Law School, Hamburg). Their work, "Social aspects (working conditions and consumer protection) of the digital economy in the mobility sector: a challenge for regulation", is focused on a specific sector, transport markets, of a huge economic importance and in which digital intermediation has achieved a significant degree of maturity, thus bringing it

to the forefront of conflict. In addition to a precise dissection of the regulatory situation, the analysis includes a very interesting call for solutions through more and more demanding self-regulation.

More transversal is the work of another of us (Alba Soriano Arnanz, Universitat de València: "La propuesta de Reglamento de Inteligencia Artificial de la UE y los sistemas de alto riesgo"), which focuses on analysing how, at the European level, an increasingly demanding regulatory model is being constructed for the uses of artificial intelligence and the various algorithmic tools that these large platforms use, in an increasingly refined and precise manner, for their intermediation and processing of information on users, their preferences and the functioning of the markets in which they operate. Focusing on the analysis of the recently presented proposal for the EU Regulation on Artificial Intelligence, the study dissects the specific high-risk problems, the mechanisms envisaged to control them and assesses their viability and sufficiency.

In addition to these first papers, which focus more on the structure of these markets, their regulation and the dynamics of competition, a second block of papers analyses in detail and rigour some of the problems more closely linked to the dynamics of private law, relations between platforms and between platforms and consumers. These works begin with the article by Mireia Artigot Golobardes (Universitat Pompeu Fabra, Barcelona) on automated contracting, which raises the limits that traditional contract law and the current data protection legal framework present when dealing with algorithmic contracting and, in particular, when protecting weaker parties (“Las inherentes limitaciones del modelo autodeterminista de protección de datos en Europa”).

Along the same lines, but starting from the definition of the problem and seeking solutions, Sébastien Fassiaux (Universitat Pompeu Fabra, Barcelona) proposes possible solutions that involve, precisely, combating some of the problems that may be a consequence of the transformations brought about by technology with technological solutions and, specifically, establishing as legally necessary in a series of cases default systems, directly derived from the design of the platform and its programming, which determine greater privacy.

Completing these reflections, María L. Mena (King's College, London) presents an interesting reflection on some of the consequences of the so-called "smart contracts" and the use of technologies such as blockchain and distributed registration systems in general, highlighting the challenges they pose in the contract formation phase in her paper "Towards the dehumanization of the contract formation phase. Algorithmic contracting and smart contracts".

Edoardo Vinchesi (Università Ca'Foscari, Venice) closes this block with his paper "The social network profile shutdown in the digital identity perspective", which analyses recent

judicial decisions in Italy. The paper analyses recent court decisions which, in Italy, have recognised the cancellation of digital profiles without justification as grounds for the recognition of compensation for non-pecuniary damages (in accordance with article 2059 of the Italian Civil Code), as it is understood that these decisions, if they have not been correctly and thoroughly agreed by the parties, may represent a clear example of abuse on the part of the platforms towards their clients and consumers.

Finally, Akihisa Hirano and Victoria Granda (Universitat de València) close the monograph with a case study on the effects of the digital economy as a factor of inequality, analysing the first data on the consequences in two very different economies in the Pacific region, Japan and Peru. Their paper "Digital divide as an inequality factor. A study for the digital future in the Pacific Region" provides very interesting data in this respect and a different perspective on the adaptation of different societies and development models to the effects and transformations caused by the digital economy, which must lead to different regulatory strategies to combat inequality.

In our opinion, all the papers presented provide a very interesting immersion into some of the problems, whether related to the necessary regulation of these markets from a public-legal perspective or in terms of competition law and the prevention of abuses of dominant positions, whether they are defined on the basis of the particularities of the new digital intermediation markets, whether they are related to the conflicts generated by some of their instruments (such as algorithms and artificial intelligence) in their different modalities, or whether they refer to questions of contracting with consumers and the protection of the weaker parties in the legal relationships that arise in these markets. We hope that it will be interesting and, above all, useful reading for the readers of the Journal and, more generally, for all those interested in the study of these issues.

València, 2 November 2021

Andrés Boix Palop and Alba Soriano Arnanz
Lecturers in Administrative Law
University of Valencia

The publication of this monograph has been made possible in part thanks to the support of the Erasmus Programme of the European Union, channelled through the Jean Monnet Network "Sharing Economy and Inequalities across Europe" (611585-EPP-1-2019-1-ES-EPPJMO-NETWORK).

With the support of the Erasmus+ Programme of the European Union

DIGITAL PLATFORMS COMPETITION REGULATORY CHALLENGES

Por

ANDRÉS BOIX-PALOP
University of Valencia

Andres.Boix@uv.es

Revista General de Derecho de los Sectores Regulados 8 (2021)

ABSTRACT: The massive reduction of costs due to efficient platform brokerage has allowed the “collaborative commons” to expand and evolve, and also to create new and very efficient markets: the so-called “sharing economy” and more broadly, the (digital) platform economy. However, bigger and more efficient sharing platforms also have some drawbacks, such as the concern that these powerful digital brokers could harm fair competition. Nevertheless, economic models centered in microeconomic consequences seem to support the idea that digital platforms have rarely inhibited the emergence of competitors, nor do they seem to be extracting predatory benefits by abusing their position to the detriment of consumers. This relative lack of risk, when we use an “only economic approach”, has pushed competition authorities across Europe to promote the new so-called collaborative business models, regardless of other potential risks: not only the competitive risks at a macroeconomic scale, but also the social ones. Both deserve greater and more careful analysis. In order to produce such an analysis, it would be necessary for the competition authorities to be institutionally reshaped and reinforced with different types of staff. Also, a more ambitious vision of the competitive issues, combinng both economic and social issues, would be required.

KEYWORDS: digital economy, digital platforms, sharing economy, legal change, competition, two-sided markets, digital brokerage.

SUMMARY: I. Digital economy, platform brokerage and network externalities. 1. Digital economy and platform brokerage. 2. The question of scale in digitally brokered markets. 3. Network effects and platform brokerage. II. Natural monopolies and digital brokerage. 1. A revision of the natural monopoly conditions applied to digital brokerage. 2. A revision of the theoretical model of competition in platform markets and its actual effects. 3. Is the traditional approach of European competition authorities still valid for digitally brokered two-sided markets? III. Outlining a better approach to deal with the new risks of digital brokers’ anticompetitive behavior in two-sided markets. 1. The challenges faced by a new economic approach for competition regulation in the sharing economy. 2. Some conclusions about possible changes in the goals and institutional design of competition authorities. IV. List of PAPERS AND works mentioned in this paper.

PLATAFORMAS DIGITALES, COMPETENCIA, RETOS REGULATORIOS

RESUMEN: La gran reducción de costes consecuencia de la eficiente intermediación que facilitan las plataformas ha permitido por un lado que el llamado "procomún colaborativo" se expanda y evolucione, madurando, pero también que aparezcan mercados nuevos y muy eficientes: la llamada "economía colaborativa" y, más ampliamente, la economía de las plataformas (digitales). Ahora bien, las ventajas de estas plataformas de intercambio en términos de una mayor eficiencia conllevan necesariamente algunos inconvenientes, de entre los cuales destaca el enorme poder que su posición central como intermediaros les puede conferir y la preocupación

derivada de ello de que, dado su creciente poder como intermediarios digitales, puedan perjudicar la competencia. No obstante, los modelos económicos centrados en cuestiones microeconómicas parecen respaldar la idea de que las plataformas digitales rara vez han inhibido la aparición de competidores, así como tampoco tienen sencillo extraer beneficios predatorios abusando de su posición en detrimento de los consumidores. Esta relativa falta de riesgo a partir de análisis basados en el mero análisis de la eficiencia económica ha empujado a las autoridades de competencia de toda Europa a promover los nuevos modelos de negocio "colaborativo", sin tener en cuenta otros riesgos potenciales: no sólo los competitivos a una escala macroeconómica, sino también los sociales. Ambos merecen un mayor y más cuidadoso análisis. Para realizar dicho análisis, sería necesario que las autoridades de la competencia se remodelaran institucionalmente y se reforzaran con distintos tipos de personal. Asimismo, sería necesaria una visión más ambiciosa de las cuestiones de competencia, que combine tanto las cuestiones económicas como las sociales.

PALABRAS CLAVE: economía digital, plataformas digitales, economía colaborativa, cambio legal y transformación tecnológica, competencia, two-sided markets, intermediación digital.

I. DIGITAL ECONOMY, PLATFORM BROKERAGE AND NETWORK EXTERNALITIES

1. Digital economy and platform brokerage

Many things have already been said about the so-called *platform economy* (sometimes also called "sharing economy", especially when underlining the sharing dimension of the phenomenon and its social effects). Beyond enthusiasm and rhetoric, which are both fairly common around the subject - and not always free of subjective interests or biases-, we may be in a better position to focus on the fundamental changes produced by this kind of economic exchanges if we try to fully understand their implications from a legal and competitive perspective. Thus, we can define the platform economy/sharing economy, in very broad and general terms, as transactions that take profit of pre-existing resources that were not being used to the maximum degree because of the inherent difficulties in matching capacity (supply) and necessities (demand)[1]. Some of these difficulties have been sorted out by new technological developments that have enhanced the access of both sides to any transaction to all the information available about possible counterparties through digital intermediation platforms[2].

We can focus our attention on different aspects of these changes. A lot has been written, for instance, about the true "collaborative" nature of the exchanges fueled by

[1] The so-called sharing economy is also said to be linked to the emergence of new social trends that are less anchored to an ownership mentality (BOTSMAN, Rachel & ROGERS, Roo (2010): *What's mine is yours: the rise of collaborative consumption*, New York, Harpers Collins Publishers, pp. 97-108).

[2] PARKER, Geoffrey G.; VAN ALSTYNE, Marshall W. & CHOUDAR, Sangeet Paul (2016): *Platform Revolution. How networked markets are transformating the economy and how to make them work for you*, New York, Norton & Company, pp. 16-33.

digital platforms, their positive cultural aspects[3] and their capacity to trigger substantial transformations in the global economy from radically optimistic visions[4]. Praise has often been given to the supposed non-commercial approach involved[5]. Many supporters of the phenomena have explained the environmental advantages of replacing individual property ownership of some goods with common shared use[6] to reduce idle capacity, pointing this out as a key feature of the sharing economy[7]. But, in the end, the critical factor that explains what we are seeing is that digital brokerage using Internet platforms, i.e. new market intermediation technology, is reshaping, in a far more effective way, how we exchange goods and services. Accurate digital brokers are allowing not only sharing activities in which non-professionals are involved, but also the emergence of new commercial activities that are explicitly focused on making profits that can only fit into the category of "collaborative" activities with difficulty[8]. Nevertheless, attempts to separate them from the non-economically-oriented activities or from the uses that merely try to reduce the idle capacity of pre-existing goods risk being not only difficult, but artificial. The boundaries are blurred, if they exist at all.

In fact, focusing the analysis on how new technology has enhanced platform brokerage in recent years, matching supply and demand with lower costs and better accuracy, is the better way to analyze the phenomenon from a legal perspective. This is because the fundamental changes that could trigger a different legal response are all closely related to this aspect of the economic transformation[9], which is derived from the extension of the uses of the sharing economy and digital platforms' activities[10]. If intermediation between suppliers and consumers are studied by themselves, regardless of the other aspects involved in the business, a clearer image of most of the legal problems we face in relation to the so-called platform economy appears. These problems are mostly the same, regardless of whether those activities are clearly professional, full-time and profit-oriented, or not. Focusing on the changes introduced by new technologies

---

[3] AIGRAIN, Philippe (2012): *Sharing culture and the economy in the Internet age*, Amsterdam, Amsterdam University Press, pp. 27-43.

[4] RIFKIN, Jeremy (2014): *Zero marginal cost society. The Internet of things, the collaborative commons, and the eclipse of capitalism,* New York, St. Martin's Press, pp. 1-25.

[5] BOTSAM & ROGERS (2010: 41-59).

[6] RIFKIN (2014: 225-254).

[7] BELK, Russell (2007): "Why not share rather than own?", *The annals of the American Academy of Political and Social Science*, available on the internet at: http://ann.sagepub.com/content/611/1/126 (last accessed on 27 September 2021).

[8] As for "sharing for profit", see DYAL-CHAND, Rashmi (2015): "Regulating Sharing: The Sharing Economy as an Alternative Capitalist System", 90-2 *Tulane Law Review*, pp. 251-259.

[9] EVANS, David S. & SCHMALENSEE, Richard (2016): *Matchmakers*, Boston, Harvard Business Review Press, pp. 19-20.

[10] PARKER, VAN ALSTYNE & MARSHALL (2016: 16-33).

in platform brokerage will allow us to cover, from a competitive point of view, all the phenomena and the legal challenges posed by the leverage position gained by these new and powerful brokers, notwithstanding the actual links between the brokers and their clients. This means that for the purpose of an analysis of the competitive and legal challenges, the positions of intermediaries such as Google or Amazon, Uber or Airbnb, Blablacar or Craigslist will be quite comparable, as long as they act in similar terms as digital brokers. The key issue, from this perspective, will be the leverage capacity generated by their key position in two-sided markets. The types of clients or counterparties these platforms have can be professional and business-oriented, individuals who are trying to reduce idle capacity or communities promoting sharing values for ideological or environmental reasons. From a competitive perspective, this makes no essential difference.

To complete this first part, it would be useful to do a quick recap of a few of the facts related to some of the economic effects produced by technology in recent years. Digital platforms have enhanced brokerage at an incredible but steady pace -which also means, almost certainly, that we will see even more improvements in the coming years[11]. The emergence of important economies of scale, the reduction of waste, better pricing precision, more dynamic information about the market, among other things, are only some of the effects that we can already take for granted[12]. Better brokers are not only able to determine where you can find what you need -or where you can find buyers for the goods or services you offer- but also to do it very quickly, immediately matching supply and demand, and allowing both parties to the exchange to do it by themselves with consumer-friendly interfaces. These digital intermediation platforms, once they have been developed, can also be offered at no cost at all to their users/clients/counterparts if web-placed publicity covers the costs, or at least, at a very reduced price (excluding the cost of the hardware or device you must use and the cost of the connection to the Internet). The massive reduction of costs due to efficient platform brokerage may affect, little by little, almost any market: that is how the so-called “collaborative commons” could lead us to a “near zero marginal cost society”[13], according with some views, while others see in the reduction of marginal costs and the scale of foreseeable profits a path paved with big competition issues because of the very structure and scale allowed by the

[11] ZURIMENDI ISLA, Aitor (2020): “Naturaleza jurídica de las plataformas digitales”, *Revista General de Derecho de los Sectores Regulados*, nº 6.

[12] LOBEL, Orly (2016): “The Law of the Platform”, 16-212 San Diego Legal Studies Paper, *Minnesota Law Review*, pp. 14-20.

[13] RIFKIN (2014: 69-87).

platform economy[14] (for the moment, the analysis of most scholars and competition authorities has considered, though, that the very fact of producing "losers" in market competition because of this scale and efficiency issues does not mean that we can identify legal objections from a classic Competition Law analysis[15]).

2. The question of scale in digitally brokered markets

Digital brokerage creates a new scale for exchanges of goods and services. A scale that is, in some markets, e.g. the provision of digital services, potentially global. But even in goods markets, these platforms, which are associated with better distribution, can expand the scale to a point unknown to date, allowing producers or retailers to reach consumers at any corner of the world. In those fields, though, the digital platform intermediates in a way that is not very different from the position of traditional retailers. Nevertheless, because it is able to reduce costs for both sides -suppliers and demanders- through better brokerage service, the digital broker, or the sharing economy platform, will have extensive opportunities to generate business.

We already know that, even in markets or exchanges where it is not possible to go global, e.g. services that must be provided or conducted in person, better brokerage also increases the size of the market and enhances transactions. That is the reason why the so-called platform economy has evolved in so many areas, from personal exchanges aimed at reducing waste and using idle capacity to the emergence of new professional markets. As long as brokerage is made better -and the network bigger, thus reducing transaction and information costs[16], new market niches will appear. This evolution is hardly avoidable. It has been seen in every economy field because the network exchange in question has evolved, increased in size and then matured. For instance, the use of idle capacity in automobile mobility has matured from car-sharing pools that have allowed users to save money by optimizing the use of their cars to a market in which better brokerage technology allows even more efficient matches, thus promoting the emergence of professional brokers. They display cutting edge technology that allows them to expand their networks, creating efficiency that they can then translate to consumers. As the markets mature and the demand consolidates, a wide range of suppliers are established, including professionals that are not "sharing" idle capacity, but instead are offering services that take advantage of the enhanced matched capacity of the broker to create a

[14] ZALE, Kellen (2018): "Scale and the Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 45-50.

[15] DUNNE, Niamh (2018): "Competition Law in the Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 104-107.

[16] EVANS & SCHMALENSEE (2016: 65-66).

business offering the requested services. This evolution has been the same -or very similar- in every market, from the well-know examples of car mobility[17] markets and peer-to-peer accommodations -especially short-stay rental markets[18]-, in which the enhancement of digital brokerage has led to a mature market to almost any other market today, thus generating an increasingly market share for the so-called "gig-economy" in many services markets, with very special features directly connected to this business-architecture (e.g. in relation to the organization of work within these companies[19]).

There is a similar pattern in the emergence of new market niches and the inevitable consolidation of business-oriented brokerage platforms in those markets, coping with the exchange market with the non-professional actors that were at the origins of the sharing economy. Naturally, similar patterns lead to risks that are also very much alike, which thus produces comparable legal challenges. The economic maturity of those markets then forces our legal system to react, establishing some rules; however, this reaction is not always necessary where the sharing economy has not yet reached such a stage. First, tax issues have arisen in those market niches, but they may be circumvented when the exchanges are still made at a more reduced scale. Once they have grown, governments must tax sharing activities, although they could try to make it easier[20]. The maturity of the market, i.e. its own development, also makes another big difference:

---

[17] DOMÉNECH PASCUAL, Gabriel (2015): "La regulación de la economía colaborativa (El caso "Uber contra el taxi")", 175-176 *CEFLEGAL*, pp. 61-104, with an exhaustive analysis of the complete literatura on the subject. Lately, see also on this same topic GONZÁLEZ CABRERA, Inmaculada (2020): "Taxis y VTCS/PHVS (*Private Hire Vehicles*) en España en el Reino Unido. Una visión crítica de las regulaciones desarrolladas en las áreas metropolitanas de Barcelona y de Londres", *Revista General de Derecho de los Sectores Regulados*, nº 5. On the regulative reaction across diffferent countries, NOGUELLOU, Rozen & RENDERS, David,(eds) (2018): *Uber & Taxis. Comparative Law Studies*, Brussels, Bruylant. See also my take on the issue and its conflict with traditional Spanish public service regulation at BOIX PALOP, Andrés, (2017): "La ordenación del transporte urbano colaborativo", Boix, De la Encarnación & Doménech (eds.), *La regulación del transporte colaborativo*, Aranzadi - Thomson Reuters, pp. 119-152. More recently, see the recapitulation by MITCHELL, Matthew D. & KOOPMAN, Christopher (2018): "Taxis, Taxis and Governance in the Vehicle-For-Hire Industry", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 78-90.

[18] DE LA ENCARNACIÓN VALCÁRCEL, Ana María (2016): "El alojamiento colaborativo. Viviendas de uso turístico y plataformas virtuales" *5 REALA (Revista de Estudios de la Administración Local y Autonómica),* available on the internet at: http://revistasonline.inap.es/index.php?journal=REALA&page=article&op=view&path%5B%5D=10350 (last accessed on 1 October 2021). See also my take on the issue at BOIX PALOP, Andrés, (2018): "Estrategias regulatorias para la resolución de los conflictos de intereses generados por la proliferación del alojamiento de corta duración con intermediación digital" in De la Encarnación (dir.) *La regulación del alojamiento colaborativo,* Aranzadi - Thomson Reuters, pp. 261-293.

[19] VALLAS, Steven & SCHOR, Juliet B. (2020): "What Do Platforms Do? Understanding the Gig Economy", Annual Review of Sociology, 46, pp. 273-294, available on the internet at: https://doi.org/10.1146/annurev-soc-121919-054857 (last accessed on 1 October 2021).

[20] WOSSKOW, Debbie (2015): *Unlocking the sharing economy. An independent review. Report to UK Business Minister,* 2015, available on the internet at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378291/bis-14-1227-unlocking-the-sharing-economy-an-independent-review.pdf (last accessed on 1 October 2021).

When there are substantially more exchanges, the social risks that could be ignored until that stage should finally be taken into account. In fact, scale also matters in that sense, because substantial social risks appear only when the sharing activity reaches a certain scale. It is only after this tipping point has been reached when new regulations appear: as a reaction, for instance, to annoyances to neighbors arising from a well-developed short-term rental market[21], soaring prices for accommodation[22], environmental effects[23], etc.

When we analyze the initial response of the different regulatory bodies across Europe, we can see that these concerns are indeed present. However, the main interest of the agencies in continental Europe has been, at least initially, how to deal with big disruptions in some previously regulated markets. This has been the case at the OECD level[24], as well as in countries like Germany[25], Spain[26], and France[27], among others. Only after

[21] DE LA ENCARNACIÓN VALCÁRCEL (2016).

[22] Soaring prices for accommodation, derived from the restriction of the supply of long-term rental offers due to the increasing profit that digital brokers have helped to extract by reducing transaction costs for short-term or vacation rentals, has been identified as a negative consequence of the success of the sharing economy in cities like New York or Berlin. The latter is even considering a total ban on the activity in order to preserve the traditional rental market for the disposal of the inhabitants of the city. On the so-called "*Zweckentfremdungsverbot*", see "Wie viel Airbnb geht noch? Darf ich mein Gästezimmer in Berlin noch bei Airbnb anbieten? Darf ich meine Wohnung vermieten, wenn ich im Urlaub bin? Und was genau ist eigentlich Zweckentfremdung?", available on the internet at *Die Zeit* from April the 28th http://www.zeit.de/entdecken/reisen/2016-04/airbnb-berlin-gesetz-ferienwohungen (last accessed on 27 November 2020).

[23] The environmental issue, in general terms, is considered to be an advantage of the sharing economy, because it allows a better use of pre-existing idle capacity. It could be otherwise, though, if increased efficiency in car-sharing induces more people to use cars instead of mass transportation. It is not clear, for example, if Uber is creating more traffic in cities like New York: "Is Uber Making NYC Rush-Hour Traffic Worse?", available on the internet at *Five Thirty Eight*: http://fivethirtyeight.com/features/is-uber-making-nyc-rush-hour-traffic-worse (last accessed on 27 September 2016). See also "Uber isn't making New York City traffic any worse" available on the internet at Business Insider: http://www.businessinsider.com/uber-not-making-nyc-traffic-worse-2016-1 (last accessed on 27 September 2016). But, in the end, it has been considered that some restrictions are wise enough in order to limit congestion and address environmental issues. See BOIX PALOP, Andrés (2020a): "The Challenges of Urban Mobility and the New Urban Agenda", *Law and the New Urban Agenda,* New York, Routledge; BOIX PALOP, Andrés (2020b): "Local Leadership and Its Limits in the Deployment of Sustainable Mobility Policies", Finck, Lamping, Moscon & Richter (eds.), *Smart Urban Mobility*, Berlin, Springer, pp. 81-98.

[24] OECD (2010): *The economic and social role of Internet intermediaries*, available on the internet at: https://www.oecd.org/internet/ieconomy/44949023.pdf (last accessed on 1 October 2020).

[25] BUNDESKARTELLAMT (2010): *Competition in the "New Economy". The Internet, the new driving force,* available on the internet at: http://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/Competition%20in%20the%20New%20Economy.pdf?__blob=publicationFile&v=2 (last accessed on 1 October 2020).

[26] CNMC - Comisión Nacional de los Mercados y la Competencia (2016): *Estudio sobre los nuevos modelos de prestación de servicios y la economía colaborativa. Resultados preliminares*, available on the internet at: https://sites.google.com/site/rprelim/ (last accessed on 1 October 2020).

[27] BERBEZIEUX, Philippe & HERODY, Camille (2016): *Rapport au Premier Ministre sur l'Économie Collaborative,* Paris, La Documentation Française, available on the internet at:

those first effects more or less settled, analyzed and regulated, our authorities began to realize that other issues may require also their attention and some regulation: the effects on job-markets and workers' precariousness that the so-called gig economy may induce[28], the analysis of possible risks and biases affecting individuals due to the extensive and pervasive use of personal data and algorithms to take advantage of this huge amount of raw personal information after its conversion in market profiles[29] and, finally, competition implications that may go further strict market efficiency (as we will develop later).

To sum it up, bigger and more efficient platforms favor matches, thus facilitating transactions and creating networks that evolve and improve even more. As we can see, the entire process has features of a typical virtuous cycle… as well as some drawbacks that require new and better regulation beyond a certain point[30]. One of these major drawbacks is the concern posed by these powerful digital brokers and hegemonic platforms in terms of competition.

3. Network effects and platform brokerage

From the standpoint of network effects, the economic transformation associated with better brokerage is not negligible, nor are its implications for competition:

- Better brokerage not only allows networks to appear where they did not previously exist because the transaction costs were so high that it was impossible, but also, for the same reasons, i.e. the reduction of costs and the time, money and

---

http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/164000100.pdf (last accessed on 1 October 2020).

[28] GRAHAM, Mark & ANWAR, Mohammad Amir Niamh (2018): "Two models for a Fairer Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 328-340; VALLAS & SCHOR (2020).

[29] SCHOENBAUM, Naomi (2018): "Intimacy and Equality in the Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 459-470. On how to prevent those risks and the insufficiencies of a mere Data Protection approach as the commonly deployed within the European Union, see SORIANO ARNANZ, Alba (2021a): *Data protection for the prevention of algorithmic discrimination. Protecting from discrimination and other harms caused by algorithms through privacy in the EU and US: possibilities shortcomings and proposals*, Cizur Menor, Aranzadi-Thomson Reuters. Also, on data gathering and biases, SORIANO ARNANZ, Alba (2021b): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, nº 56; SORIANO ARNANZ, Alba (2021c): "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Teoría y Método. Revista de Derecho Público*, Vol. 3(2021) available on the internet at: https://doi.org/10.37417/RPD/vol_3_2021_535 (last accessed on 30 October 2021). Regarding to the new European proposal about a new legal framework for the use of AI in Europe, see SORIANO ARNANZ, Alba (2021d): "La propuesta de reglamento de inteligencia artificial de la UE y los sistemas de alto riesgo", *Revista General de Derecho de los Sectores Regulados*, nº 8.

[30] RANCHORDÁS, Sofia (2015): "Innovation experimentalism in the age of the sharing economy", 19:4 *Lewis & Clark Law Review*, pp. 871-924.

skills involved, it improves and expands the pre-existing networks. As any network appears, expands, or improves, more and more items, capacities, goods, or services will be offered, thus making the network even more attractive and competitive. This result, in economic terms, is essentially the same for business-oriented platforms that it is for any social network with no interest other than matching particular offers: the efficiency of the network will be increased as it attracts more users, and users will be attracted by better brokerage, thus making it even more efficient. Where the network externalities are well known and extensively documented[31], efficient platform brokerage is only a powerful catalyst of it[32].

- This effect will reduce costs even further, simply because the bigger a network is, the lower the users' effort will be to find better matches. There are clear economies of scale and associated network effects that are enhanced by the fact that digital brokerage in two-sided markets allows the enhancement of economies of scale on both the supply and demand sides[33].

- Of course, as has been repeatedly explained by all the apologists of the digital economy, the more complete a network is, the better it will optimize idle capacity[34]. The key issue here, as has been noted, is the density of the network. The denser the network is, the more the connections will become actual transactions[35]. This effect is the same for every network, whether it is business-oriented or not. The only difference is that the reduction in the waste of capacity and the optimization of idle surpluses will be translated into better services and exchanges for participants in the networks that are not business-oriented, while professional brokers will intend to extract it as a benefit of their activity. This benefit could reduce the net outcome for their counterparties: the participants in both sides of the brokered market. That is precisely the main reason why professional brokers, in order to survive, must offer more efficient brokerage than the online exchange platforms created and maintained by users or communities with no intention of making money, thus reducing the potential benefit. The network effects in digitally-brokered

[31] ECONOMIDES, Nicholas (1996): "The Economics of Networks", 14 *International Journal of Industrial Organization*, pp. 673-699.

[32] EISENMANN, Thomas; PARKER, Geoffrey & VAN ALSTYNE, Marshall W. (2006): "Strategies for Two- Sided Markets", 84-10 *Harvard Business Review,* available on the internet at: http://www.hbs.edu/faculty/Pages/item.aspx?num=22459 (last accessed on 6 October 2021).

[33] PARKER, VAN ALSTYNE & CHOUDAR (2016: 106-115).

[34] PARKER, VAN ALSTYNE & CHOUDAR (2016: 108-115).

[35] MOAZED, Alex & JOHNSON, Nicholas L. (2016): *Modern monopolies. What it takes to dominate the 21st-Century Economy*, New York, St. Martin's Press, p. 171.

two-sided markets are, for this reason, at least according to mainstream economic doctrine, somewhat difficult to transform into benefits derived by an abuse of a dominant position[36]. We will return to this point later, because if the actual evolution of the digital economy and the two-sided markets confirms this preliminary idea, then the regulatory strategies, from a competition point of view, should take it into account and thus should be different than the traditional ones (we may focus not only in problems in terms of market efficiency and consumer well-being, as the European Competition authorities and traditional analysis tend to do[37], but covering also other considerations beyond the dominant competition more economic approach that may include social costs and other effects).

The scale effects in platform markets are now being studied -sometimes in a broader and more generic manner, otherwise, market by market- by several researchers in almost every country[38]. Surprisingly, concerns related to the competitive position of the new brokers and the various sharing platforms that have emerged have been given less attention in spite of the fact that, as explained, the scale and network effects are key issues in the construction of this new market niche. They could indeed result in competitive risks that should be addressed by our legal systems. Having established how the sharing economy naturally evolves towards very competitive two-sided markets, we need to understand how important scale is for the brokers and how the sum of all these factors leads to huge network effects, as these are the most obvious risks to competition in this evolution.

We already know that regulators tend to react only when those markets have reached maturity and have acquired the size and scale that could create social risks or affect the traditional regulation of some markets. Competition concerns arise only subsequently, following a familiar pattern: the analysis of whether the new hegemons that are the result of the big network effects in two-sided markets could be deemed to be a competitive risk. We will assess the actual risk in the sharing economy of having natural monopolies as a consequence of the features of digital brokerage. In our opinion, that kind of competitive risk has been, for the moment, overstated by regulatory agencies, while other anticompetitive results of the growing power of digital brokers may have been neglected.

[36] WEYL, E. Glen (2010): "A Price Theory of Multi-sided Platforms", 100(4): *American Economic Review*, pp. 1642-1672.

[37] SCHMIDTCHEN, Dieter; ALBERT, Max & VOIGT, Stefan (2007): "The More Economic Approach to European Competition Law", 24 Conferences ion new Political Economy, Tübingen, Mohr Siebeck; DUNNE (2018).

[38] MILLER, Stephen R. (2015): "First principles for regulating the sharing economy", 53 *Harvard Journal of Legislation,* pp. 171-202.

Assessments of the risks of the sharing economy by scholars thus far, notwithstanding how rich and complete they could have been[39], have also tended to overlook this problem. At least until recent times[40].

II. NATURAL MONOPOLIES AND DIGITAL BROKERAGE

1. A revision of the natural monopoly conditions applied to digital brokerage

The main disruptions that could be caused, in competitive terms, by the new and more efficient digital brokers are, as we have seen, closely associated with the benefits derived from the network effects that were explained above. If it is true that more efficiency leads to a better and bigger network, leading to even more efficiency and thus creating a virtuous circle, then we can expect that some, if not all, of the traditional concerns raised by natural monopolies[41] can also play an important role in dealing with the competitive risks in the sharing economy[42].

Natural monopolies appear, without being established by a legal system, in certain kinds of markets with special characteristics that have been well identified and studied for years. It is common knowledge that the main factors that could lead to natural monopolies are economies of scale, sunk costs and network effects[43]. Internet platforms are an obvious example of businesses in which the network effect is huge, as explained above. It is worth remembering that the efficiency of the brokerage is closely linked to the extension of the network[44]. This network effect also leads to important economies of scale, as has been shown by the activity and consolidation of any of the major digital brokers, not only in the so-called "sharing economy" (Uber, Airbnb, etc.), but also in other fields with the same economic structure (Google or even Amazon are also digital brokers in two-sided markets). Growth is considered to be essential in those markets, to the point that most of these companies -and also their investors- prefer to use their revenue to invest in new developments or acquisitions of competitors in an attempt to consolidate a

---

[39] DYAL-CHAND (2015: 241-309), DUNNE (2018).

[40] Lastly, some of the ideas that we will cover in this work have emerged, even though still with a certain shyness, at the 2019 Report of the UNITED KINGDOM COMPETITION EXPERT PANEL (2019): Unlocking digital competition, available on the internet at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf (last accessed on 20 October 2021).

[41] POSNER, Richard A. (1968): "Natural Monopoly and Its Regulation", 21 *Stanford Law Review*, pp. 548-643.

[42] PARKER, VAN ALSTYNE & CHOUDAR (2016: 204-212).

[43] WOLF, Dieter (1999) "La réforme des services publics en Allemagne", Jean-Marie Chevalier and Ivar Ekeland and Marie-Anne Frison-Roche (eds.), *L'idee de service public est-elle encore soutenable?*, Paris, P.U.F., pp. 11-20.

[44] PARKER, VAN ALSTYNE & CHOUDAR (2016: 204-212).

position of dominance in the market, rather than to generate and cash actual profits (at least, in the first years of the race towards a dominant position as the platform of reference in each market)[45]. So, on the one hand, we have the first sign indicating that we may have a competition issue here[46]. And it is a non-negligible one.

On the other hand, though, the sunk costs are extremely low in digital brokerage[47] -almost everything any company needs to create such a platform could be reused or sold, with perhaps the only exception being the specific software development- and the cost of the technology and investment required to enter those markets is shrinking year by year at a steady rate -as it has been also the case throughout the telecommunications market[48]. In fact, digital brokerage markets are closely related to the telecommunications markets, and compared to them, are even more protected from sunk costs, as the infrastructure investment required is lower for digital brokers. Interestingly, more than a decade ago, European Union authorities considered that the telecommunications market was the natural monopoly through which technology had most transformed the conditions of competition more intensively, thus allowing market conditions in which the trend towards monopoly was not granted, precisely because of the importance of new technology[49]. This trend has only accelerated in past years. In fact, it seems that when it becomes sufficiently advanced, technology could cause the whole theory of natural monopoly to be questioned[50]. It may be that the supposed "natural" trend towards "monopoly" in some cases may only be a temporary situation that will disappear as soon as the technology is sufficiently advanced.

This is perhaps the reason that explains why the typical features of natural monopoly markets, such as the "first pass the post" or "winner takes it all" effects, do not necessarily

---

[45] Most prominent companies in the so-called *sharing economy* markets are not making money for the moment, with the prominent example of Uber, as it was the case for years for other Internet hegemons such as Amazon. See about this strategy EVANS & SCHMALENSEE (2016: 69-83).

[46] BADEN-FULLER, Charles & HAEFLIGER, Stefan (2013): "Business Models and Technological Innovation", 46-6 *Long Range Planning*, pp. 419-426.

[47] ROCHET, Jean-Charles & TIROLE, Jean (2003): "Platform Competition in Two-Sided Markets", 1-4 *Journal of the European Economic Association*, pp. 990-1029, available on the internet at: http://www.rchss.sinica.edu.tw/cibs/pdf/RochetTirole3.pdf (for the pages indicated in the footnotes, we use the version published online by IDEI, Toulouse).

[48] SRINAGESH, Padmanabhan (1998): "Internet Cost Structures and Interconnection Agreements", McKnight and Bailey (eds.), *Internet Economics*, Cambridge, The MIT Press, pp. 121-154. See also PROSSER, Tony (2005): *The Limits of Competition Law,* Oxford, Oxford University Press, pp. 177-186.

[49] European Commission Green Paper of 21 May 2003 on services of general interest.

[50] DILORENZO, Thomas J. (1996): "The Myth of Natural Monopoly", 9 (2) *The Review of Austrian Economics* (1996), available on the internet at: https://mises.org/library/myth-natural-monopoly-0 (last accessed on 6 October 2020).

apply to the digital brokerage markets[51]. In fact, in any of the so-called sharing markets in question, we can hardly find companies that were market-leaders in those markets before the current hegemons appeared. Google, Amazon, Facebook, and even Uber and Airbnb were not the first companies to offer digital brokerage services in their respective fields, but they succeeded by displaying better technology than the previous actors in the market[52], thus proving that competition and even the substitution of previous hegemons is not only feasible but quite common in digital markets. All of these companies had the capacity to improve the efficiency of the brokerage through better search or matching algorithms, improved software, user-friendly interfaces, etc; market innovations that led to more efficiency and a translation of those gains to the public; and they were rewarded by consumers accordingly. The key element that was always present and that explains the hegemony of each company is commonly said to have been innovation and the capacity to display and offer cutting-edge technology that mastered the multifaceted network effects and transferred those gains in efficiency consumers[53]. That is the reason why apparent monopolies can be found in the Internet brokerage markets, but they are always at risk of being replaced by others because of technological change and innovation. This shows how, in competition terms, the importance and effects of monopolies have changed in technological markets[54]. For plausible competitors, the costs of entering those markets are not prohibitive, and the possibility of making profits, even in very small specialized market niches, guarantees a diversity of possible new entrants in spite of the effects of the "long tail"[55]. Consequently, competition is at least possible in digital brokered markets, and therefore, innovation could mean that a new company with a better brokerage system could shift consumer trends and compete efficiently. As we will see next, economic models support the idea that the monopoly concern should not be the most dangerous outcome of the growing importance of digitally brokered platforms, at

---

[51] HUOTARI, Pontus; JÄRVI, Kati; KORTELAINEN, Samuli & HUHTAMÄKI, Jukka (2016): "Winner does not take all: Selective attention and local bias in platform-based markets", *Technological Forecasting and Social Change*.

[52] DE LEON, Ignacio (2016), "Competition Policies in the Internet-based industries: Do we need to reboot the debate?", *Latin American and Caribbean Competition Forum*, available on the internet at: <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2016)26&docLanguage=En> (last accessed on 1 October 2020).

[53] EVANS & SCHMALENSEE (2016: 22-30).

[54] THÉPOT, Florence (2012): "Market Power in Online Search and Social Networking: a Matter of Two-Sided Markets", *4/2012 CLES Working Paper Series University College London* (2012), available on the internet at: http://www.ssrn.com/abstract=2307009 (last accessed on 1 October 2020).

[55] ANDERSON, Chris (2006): *The Long Tail: Why the Future of Business Is Selling Less of More,* New York, Hyperion.

least in terms of strict economic efficiency and its transfer to cosumers, which has been the focus of competition authorities and regulators for decades.

2. A revision of the theoretical model of competition in platform markets and its actual effects

Regulators and scholars have had problems in using the previous knowledge regarding competition matters when dealing with those activities, in part because tech companies do not follow the behavior of typical monopolies. Rochet and Tirole have theorized since 2003 about how the network effects will affect the kind of markets in which a digital broker is placed between the two sides of the market helping both suppliers and demanders to find better matches among themselves. They described them as "two-sided markets", and they tried to understand why some of the trends in other network-based markets that led to a natural monopoly -and its inherent risks- did not seem to apply here. In their work on two-sided markets, they guessed that price allocation in that kind of market is highly affected by the crucial need for brokers to have both sides of the market in their platform[56]. They cannot risk losing them, and that is perhaps why there is always a possibility of competition[57]. The importance of the technological edge in maximizing efficiency[58], thus attracting both sides of the market, and the fact that better technology for accomplishing this could potentially be at the disposal of any possible competitor at a non-prohibitive cost, acts as barriers to the predatory tendencies that are the most dangerous outcome of monopoly situations. The threat of new entrants developing better technology or offering the same service at a lower price inhibits the temptation to take advantage of the possibility of the leverage given by their present domination of the market. Revisions made some years later regarding the evolution of those markets seem to have proven that the initial analysis was right: As far as we know, a possibility of competition always exists in two-sided markets when the critical lead depends on the efficiency of the brokerage in using technology[59].

---

[56] ROCHET & TIROLE (2003: 990-1029).

[57] PARKER, VAN ALSTYNE & MARSHALL (2016: 79-86).

[58] DEMARY, Vera (2015): "Competition in the sharing economy", Paper 19/2015 *Institut der Deutschen Wirtschaft Köln Policy*, available on the internet at: http://scholar.google.es/scholar_url?url=https://www.iwkoeln.de/_storage/asset/235443/storage/master/file/7255909/download/Sharing%2520Economy%2520Policy%2520Paper.pdf&hl=ca&sa=X&scisig=AAGBfm3Wn68Ulcwotmb8GcaKGbJZQgHMgg&nossl=1&oi=scholarr&ved=0ahUKEwj9n (last accessed on 27 September 2020). See also MONTERO & FINGER (2021: 20-25).

[59] ROCHET, Jean-Charles & TIROLE, Jean (2006): "Two-Sided Markets: A progress report", 37-3 *The RAND Journal of Economics,* pp. 645-667, available on the internet at: <https://www.jstor.org/stable/25046265?seq=1#page_scan_tab_contents> (last accessed on 1 October 2020); ARMSTRONG, Mark (2006): "Competition in two-sided markets", 37-3 *RAND Journal of Economics*, pp. 668-691.

There are other elements to be noted that reinforce this idea. The fact that, as previously underlined, most of the current hegemons were not the first digital brokers in their respective markets is one of them. But there are still other empiric developments that point in the same direction. For instance, the low range of the benefits that these companies have been achieving, even after becoming dominant, despite working in huge markets and even after realizing impressive yearly turnovers, is nothing but surprising given the large volume of business in some of these markets once they have reached maturity[60]. The threat created by emerging competitors, combined with the differences in digital broker markets that inhibit natural monopolies and reduce the possibility of abusing the leverage created by them as explained above, has consolidated a non-predatory trend in digital two-sided markets. Efficient brokers swiftly translate gains in efficiency to their counterparties -mostly to the demand side, i.e. consumers, by reducing prices or offering better services, rather than converting these gains in efficiency to improve their profit accounts for distribution to shareholders.

As a provisional conclusion, then, monopoly -or big hegemony- in digitally brokered two-sided markets does not seem to be an important competition risk in two of the most critical ways that monopolies used to be dangerous: they rarely inhibit *per se* the emergence of competitors, nor do they seem to extract predatory benefits by abusing their position, therefore linking to the limits of traditional Antitrust Law when confronting competition issues in the platform economy[61].

3. Is the traditional approach of European competition authorities still valid for digitally brokered two-sided markets?

This particular assessment of the competitive risks in two-sided digital markets is not without consequences for the regulation of the digital economy, the so-called sharing economy and digital platforms. As we have already explained, perhaps not every two-sided market can be considered as an example of the platform economy, but the economic structure of the interactions and their actual effects are very similar. In most cases, the difference lies only in a question of size and maturity. That is why we consider that we should translate the reflections made *supra* on the monopoly concerns and the

[60] For instance, Amazon only recently, during the last decade, made benefits within the US (for instance, it made US$ 100 billion in 2015, one of its best exercises, after an operating income of more than US$ 2.200 billion, a very low rate for a hegemon with a position close to a monopoly in most markets) and still today, in 2021, despite having showed its biggest performance up to date, is losing money in such a important and mature market as Western Europe. Uber or AirBnB, meanwhile, are not making profits at all at the moment, because the markets in which they operate are not mature enough. See PARKER, VAN ALSTYNE & MARSHALL (2016: 224-227).

[61] DUNNE (2018: 104-107).

network effects in digitally brokered two-sided markets to the entire analysis of the competition matters that arise in the digitally enhanced platform economy.

Given the traditional approach of the European Union competition regulation and its implementation by the European Union competition authorities, it is not surprising at all that regulators do not see many competition concerns in these new markets. They are unlikely to detect them, because their "competition only approach", as the European model has been labeled[62], or the "more economic approach" typical from US competition authorities[63], has not been designed to deal with market hegemons that behave in that way.

The European competition bodies -and its American counterparts- focus mainly on market structure questions like anti-trust issues, mergers, dominant position and so on, but only to control and eradicate situations that could present a risk to the actual possibility of new actors entering the market. They also deal with the predatory microeconomic effects that a dominant position in a market could create. Given the fact that the dominant companies in two-sided markets, such as the digital brokers that channel most of the activity in the sharing economy, tend to display a variety of short-term price rebates that clearly benefit consumers in the short term, this approach is not easily able to detect other problems that may be involved in competition matters in the sharing economy. The actual issues are rarely related to using a dominant position to skim the market and extract unfair profits from consumers or to exclude competitors. Rather, they are related to taking advantage of the leverage that a dominant position can offer to successful digital brokers, not against competitors or new entrants, but against their suppliers. The economic structure of two-sided markets makes one side (suppliers) more vulnerable than the other (consumers). Because competition tradition has neglected the vulnerability of suppliers, especially when it is indirectly derived from technological issues, the toolkit at our disposal to address it falls short. There are also other possible macroeconomic effects, as well as some social effects, which are not directly related to competition, that it may be interesting to study jointly with them, because the way in which we use competition law does indeed always internalize some social values[64].

---

[62] WIGGER, Angela (2008): *Competition for competitiveness: The Politics of the Transformation of the EU Competition Regime*, doctoral thesis available on the internet at: <http://dare.ubvu.vu.nl/handle/1871/15601> (last accessed on 1 October 2020).

[63] SCHMIDTCHEN, ALBERT & VOIGT (2007). Recently, an extensive and thoughtful analysis of the "more economic approach", with interesting conclusions and some considerations about its inherent limits that can complete Wigger's study can be found at RODILLA MARTÍ, Carmen (2018): *Los Precios Excesivos por Explotación como Ilícito del Derecho de la Competencia*, Cizur Menor, Aranzadi - Thomson Reuters, pp. 65-86.

[64] PROSSER (2005: 24-25).

To date, the preliminary studies of the challenges posed by the sharing economy, not only the first analyses at the OECD level[65], but also the abovementioned works produced by several national agencies, have failed to develop this perspective. The European Union Communication on the Collaborative Economy[66] is a very good example of everything we are saying. The analytical papers include intensive studies on market access requirements, liability issues, the possible gains in growth and the labor markets derived from collaborative models of business. This has also generally been the trend for the national competition agencies. They have essentially overlooked any competitive effects produced by the very different technological structure of those markets. The first exceptions were the "Data and Competition Law" document, produced jointly by the French *Autorité de la Concurrence* and the German *Bundeskartellamt*, which at least analyzed -correctly, though still at a very incipient stage- data collection as a very important market power tool[67], and the European Commission Consultation Report of 2015, which at least identified some of the possible problems that will be exposed later -although there has been no competition development of them[68].

Broadly speaking, because the traditional "economic only approach" aims to prevent micro-economic problems and the unfair use of leverage against consumers or competitors, the possible negative outcome of the activities of these new hegemons in relation to their counterparties has not, to date, been taken into account. This is a hardly new outcome. We have already seen a similar pattern in other two-sided markets. For instance, in a market in which at least some of most of the previously explained features of two-sided markets clearly apply, i.e. the search engines market -and all kinds of search-related features- the European Commission has finally taken some action against Google for some of its practices. Nevertheless, consumers, at least in the short term, could not have been displeased with the aggressive rebates that Google has induced and promoted for all kinds of services and goods for which it acts as a broker. Interestingly, however, the main element retained by the European Union competition authorities has

---

[65] OECD (2010).

[66] European Union Communication webpage on the Collaborative Economy. Available on the internet at: https://ec.europa.eu/growth/single-market/single-market-services/collaborative-economy_es (last accessed on 26 October 2021).

See also EUROPEAN COMMISSION (2016) COM 2016 356 final. *A European Agenda for the Collaborative Economy.* Available on internet at: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-356-EN-F1-1.PDF (last accessed on 27 September 2020).

[67] AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT (2016): *Competition Law and Data.* 10 May 2016. Available on the internet at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf (last accessed on 6 October 2020). See also PARKER, VAN ALSTYNE & MARSHALL (2016: 243-248).

[68] EUROPEAN COMMISSION (2015).

been a prejudice against Google's competitors, i.e. other search engines, mostly specialized ones[69]. Analyses of the possible negative effects on the suppliers of services that could not risk refusing the use of the broker because of the risk of being excluded from the market are, for the moment, mostly non-existent[70]. Also, macroeconomic effects, effects in other social and economic fields (as to labor relations or in the problems generated to other business or the social fabric), even though being more and more clear and an actual social and political issue[71], continue to be out of the realm of the analysis made by Competition authorities. Not surprisingly, all the analyses of sharing economy issues that have been produced by different competition bodies across Europe -not only at the European Union level, but also in the different Member States- have also neglected this approach[72].

In conclusion, due to the narrow conceptual view we have explained, competition authorities across Europe are, for the moment, limited to developing the virtues of the new collaborative business models, omitting some of their potential risks: not only the competitive risks, but also the social ones. Both deserve greater and more careful analyses. Further, such analyses should be done by the competition agencies, and in

[69] See the documents of the process on the official competition website of the European Union, available on the internet at: http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740 (last accessed on 27 September 2020). Lastly, The General Court of the European Union ruled on the 10th November 2021 (case T-612/17) in the case *Google Shopping* (Google and Alphabet v Commission) that, that, by favoring its own comparison shopping service on its general results pages through more favorable display and positioning, while relegating the results from competing comparison services in those pages by means of ranking algorithms, Google departed from competition on the merits", in a typical decision of that kind, focused in the possible harm to competitors derived from broker's privileged position (see General Court Press release on case T-612/17 at https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210197en.pdf, last accessed on 11 November 2021).

[70] CLEMONS, Eric K. & MADHANI, Nehal (2010): "Regulation of Digital Businesses with Natural Monopolies or Third Party Payment Business Models: Antitrust Lessons from the Analysis of Google", 27-3 *Journal of Management Information Systems,* pp. 43-80.

[71] For instance, in the las US Presidential Election, Law scholar and Democratic candidate Elizabeth Warren lead a public fight on the necessity of further control of big tech, including the possibility of breaking up some of the biggest digital platforms because of their market power and its social and economic (in terms of competition) consequences. The position of Elizabeth Warren candidate bid can be seen at https://2020.elizabethwarren.com/toolkit/break-up-big-tech (last accessed on 30 September 2021). Lately, the Biden's Administration, after winning the election in 2020, seems to be given some steps in this direction, the most important one being the nomination of Jonathan Kanter as Justice Department's Antitrust Chief. Kanter is an outspoken critic of the huger market power of big digital platforms, thus making possible a change in the approach of the US Justice Department in Competition issues regarding digital markets and platform economy: https://www.nytimes.com/2021/10/06/technology/biden-jonathan-kanter-big-tech.html (last accessed on 30 September 2021).

[72] See EUROPEAN COMMISSION (2015) and EUROPEAN COMMISSION (2016). The same omission can be found in the Spanish CNMC Report (2016) and in the French Report (2016). The previously cited Franco-German Report on Data Collection and Competition (2016) fails to see how essential this question is to the competitive dynamics in the sharing economy markets.

doing so, they need to work with a new conceptual framework and to use a range of legal and analytical tools richer than those currently available[73].

III. OUTLINING A BETTER APPROACH TO DEAL WITH THE NEW RISKS OF DIGITAL BROKERS' ANTICOMPETITIVE BEHAVIOR IN TWO-SIDED MARKETS

1. The challenges faced by a new economic approach for competition regulation in the sharing economy

The "economic-only approach" or the "more economic approach", which both focus on micro-economic matters, tends to minimize the competitive conflicts that are produced by increased the dominance of some digital brokers in two-sided markets, which is often the case in the hegemon digital platforms when markets in which they operate, at last, mature (for instance, consider examples such as Uber or Airbnb, which are currently in control of their respective niches, a previously stage of the dominance currently held by Amazon or Google, which are now making profits and fighting competition using their huge market power). We can indeed accept that some of the traditional competitive issues are not a source of problems in these markets, because consumers can expect rebates that translate any efficiency gains obtained by the broker and because the possibility for competition may still be there. Nevertheless, the leverage capacity produced by the large network effects in the new dominant companies in the digital economy markets causes new (or not so new, but neglected in recent decades) risks to appear. Competition authorities and market regulators should focus (or refocus) on them. It is possible to identify at least four of them, following the aforementioned European Commission Consultation document[74]: technological barriers, vertical integration[75], price fixing and other forms of leverage affecting the participants in the market.

- One of the main problems in terms of competition in digital brokerage markets or sharing economy markets is the fact that, because technology provides an edge and leverage, it could also be a possible entry barrier that could be misused to alter competition, for instance, by imposing some technological requisites (relating to networks, operating systems, etc.) on participants in the market. This may occur if these

[73] MONTERO & FINGER have explained the shortcomings of traditional competition regulatory approaches (2021: 236-239).

[74] EUROPEAN COMMISSION (2015). *Consultation on Regulatory environment for platforms, online intermediaries, data and computing and the collaborative industry*. Available on the internet at: https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud (last accessed on 27 September 2020).

[75] See RODILLA MARTÍ, Carmen (2021): "Los mercados de plataformas digitales: entre el Derecho de la Competencia y la Regulación", *Revista General de Derecho de los Sectores Regulados*, nº 8 (specifically part II.2.1)

requisites are not strictly necessary, but instead are a way to discriminate against or exclude some actors from the market; brokers may view them as desirable in order to gain or retain leverage in the specific market[76]. Regulation and the preemptive adoption of technology, as a competitive matter, have already been studied in other fields[77]. The problem we face when confronted with those kinds of anticompetitive actions in a digital economy market is that traditional competition law is ill-suited to analyze it. The assessment of competitive risk derived from technological barriers requires a powerful and holistic understanding of the market in question, not only of the legal and economic elements, but also in terms of innovation[78]. The required work needs an approach that combines legal, economic and technological knowledge, which is more complex than the current approach used by our competition authorities. This problem is not likely to disappear. The very essence of technological innovation in digital markets makes it difficult for public authorities, at any given time, to reach the level of expertise possessed by private actors.

It is therefore not easy to discriminate between genuine specifications aimed at ameliorating any actual platform, enhancing the user's experience or creating better brokerage and technological requisites with the hidden goal of distorting the market and empowering the broker. The only solution that our legal system has forged to face this challenge has been to increase the discretionary capacity of the competition authorities in assessing the markets and the competitive risks. The recent trend in the assessment of competition issues, not only digital platform markets, but in every technological market, has been to allow administrative bodies more room to maneuver[79]. This solution may be a sensible one, given the risks and challenges posed by innovation and technological evolution, but it should be implemented with better procedural controls, guided by certain basic principles that should be legally and previously established as binding on the competition bodies. Without a previously detailed framework for how this discretionary

[76] As happened, for instance, in the conflict between Amazon and Harper Collins, which is explained by RAHMAN, K. Sabeel (2015): "Consumer prices are not the only concern raised by dominant companies", 4-05-2015 *Boston Review Forum*, available on the internet at: http://bostonreview.net/forum/k-sabeel-rahman-curbing-new-corporate-power (last accessed on 6 September 2021). On competition matters related to the control of platform access, see PARKER, VAN ALSTYNE & MARSHALL (2016: 240-241).

[77] RIORDAN, Michael H. (1992): "Regulation and preemptive technology adoption", 23-3 *The RAND Journal of Economics*, pp. 334-349.

[78] In this sense, the work of the AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT (2016) is interesting, although it fails to offer a mature analysis of the question in relation to the technological barriers imposed by the platforms in two-sided markets.

[79] SCHWEITZER, Heike & PATEL, Kiran Klaus (2013): "EU Competition Law in Historical Context: Continuity and Change", Patel and Schweitzer (eds.), *The Historical Foundations of EU Competition Law*, Oxford, Oxford University Press.

power should be implemented by different staff profiles, this solution is a dangerous one and risks being inefficient[80].

- Another aspect that may pose a challenge to older competition regimes is the existence of vertical integration, as we have already pointed out[81]. When two-sided platforms vertically integrate part of the offer of services that they are also channeling on behalf of other counterparties, potential conflicts arise. We have seen this, for instance, in the various services that Google has decided to offer in concurrence with some of its users. If this also happens in the sharing markets, the competition authorities will be forced to treat that fact in a different way, as has been signaled by the European Commission (2015). A reaction would be necessary, although it is not clear what it should be. We have seen some examples in recent years in some two-sided markets that are clearly business-oriented, for instance, to Google's or Amazon's practices[82]. To date, however, the regulatory initiatives have been very tentative and have lacked a clear course of action. Nevertheless, it seems that digital platforms, by definition, do not tend to be characterized by vertical integration. In fact, if they were, it would be complicated to continue to categorize them as "sharing platforms". Think, for example, about the recent evolution of Uber and its project to have its own self-driving cars in the near future. It may be complicated to categorize that merely as a "brokerage activity". Nevertheless, the way in which that market is labeled has only relative importance. The essential issue is the need to establish new regulations, which may require a decision about whether to impose some "neutrality" duties on brokers as a service obligation controlled by public officials[83]. Using the broker as a semi-public regulator, or at least, as a private agent that collaborates with public regulation, may be even considered[84]. The struggle to define and control the intelligent infrastructure that allows more efficient matching in two-sided

[80] There are also non-negligible issues in relation with the important access barriers (and their implications, beyond privacy, for competition) consequence of the consideration of personal data as a product that can be controlled and owned by platforms. Even though it is not possible to develop this specific problem, it has to be said that the consideration of data (and specifically the data used by digital platforms) as part of the "commons" is a possible regulative solution that will have very interesting consequences, not only in relation of users' rights but also flattening the field for new competitors thus allowing more and better competition. See CARBALLA SMICHOWSKI, Bruno (2016): "Data as a common in the sharing economy: a general policy proposal", *Document de travail du Centre d'Économie de l'Université de Paris Nord CNRS UMR nº 7234*, available on the internet at: https://hal.archives-ouvertes.fr/hal-01386644/document (last accessed on 30 September 2021).

[81] See RODILLA MARTÍ (2021: part II.2.1).

[82] PARKER, VAN ALSTYNE & MARSHALL (2016: 241-243).

[83] GATA, João E. (2015): "The Sharing Economy, Competition and Regulation", *CPI Europe Column*, available on the internet at: https://www.competitionpolicyinternational.com/the-sharing-economy-competition-and-regulation/ (last accessed on 27 September 2021); RAHMAN (2015).

[84] DYAL-CHAND (2015: 285-288).

markets is an essential competitive element[85] and regulators should not be shy in participating[86].

- Digital platforms operating in two-sided markets enjoy a large amount of leverage against their counterparties, as has already been stated. They are precluded from using it for their own benefit because of competitive pressures from the outside. However, once they have gained a substantial presence in the market and can benefit from large network effects, they could always try to use it to introduce predatory conditions against at least one of their counterparties -the suppliers- in order to obtain better conditions that they could subsequently offer to the other counterparty- the consumers. The traditional analysis of the European model of competition, micro-economically and price-oriented, would not raise major concerns about that kind of demarche, considering it to be a perfect example of a well-functioning market[87]. Nevertheless, the structure of digital platforms and the way in which the network effects appear could raise objections about whether it could be an anticompetitive action, at least in some cases, against the suppliers of offers in the platform. In fact, some of these questions have already created practical problems in some platforms, such as the price fixing by Booking or Uber. Uber's price fixing also involves other problems (see below), but the Booking case is very interesting. The platform has become so essential for suppliers of hostel accommodations that it used its leverage to fix prices, imposing pricing clauses that also affect the prices of rentals made outside the platform. The administrative and legal reaction across Europe stopped Booking from continuing those practices: For instance, the famous French *loi Macron* declared any clause of that type void and explicitly authorized hotels to set the prices they wanted for their hotel rooms in any case, even for online reservations made via digital platforms[88]; competition authorities in Italy opened an inquiry that also forced Booking to change its policies[89].

Another consideration in relation with prizes and competition can be said in relation with the services offered at loss by digital platforms. In relation with prize fixation, a

---

[85] RIFKIN (2014: 193-205).

[86] PARKER, VAN ALSTYNE & MARSHALL (2016: 246-248).

[87] DUNNE (2018: 92-98); CHEN, Yiwei; HU, Ming & ZHOU, Yun (2019): "Pricing and Matching in the Sharing Economy", Hu (ed.), *Sharing Economy. Making Supply Meet Demand*, Cham Springer, pp. 137-164.

[88] MONTI, Giorgio (2015): "Competition Law and E-Commerce: Love-hate relationship?", *European University Institute*, available on the internet at: http://www.jean-monnet-coe.keio.ac.jp/references/giorgio_monti_04.pdf (last accessed on 27 September 2021).

[89] AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO (2016): Commitments offered by Booking.com: closed the investigation in Italy, France and Sweden, available on the internet at:

http://www.agcm.it/en/newsroom/press-releases/2207-commitments-offeresd-by-bookingcom-closed-the-investigation-in-italy-france-and-sweden.html (last accessed on 6 October 2016).

typical outcome of the efficiency-oriented "more economic approach" dominant in past decades has been the erosion of traditional regulations that, for in instance in some Member States as Spain and Belgium, prohibited the sales at loss because of competition concerns[90]. The effects of such a permissive approach in digital markets are far from being optimal[91]. Offering services at loss, as a matter of fact, allow platform hegemons to create a big competitive burden in new actors or possible competitors. Even though the consumer may receive part of the benefits in the short term, the leverage that the permission of such practices gives to bigger platforms should induce regulators to rethink their take on this practice.

- In fact, this capacity to use leverage against their counterparties is at the core of some of the legal problems that certain sharing economy platforms have already experienced. For instance, firms such as Uber, once they have become the dominant broker in their market, and thus, enjoy large network effects in their favor, indeed have the capacity to impose a generous bundle of conditions, not only price-related, to anyone wanting to participate in the exchange of services made via the platform. As discussed above, this high degree of leverage will not be used against consumers because of the absence of the traditional conditions for a natural monopoly. This absence would make it dangerous for the current hegemon in a market in which competition is always possible to facilitate other brokers' efforts to fill a space of inefficiency and to profit from it by making better offers and more efficient matches. Nevertheless, it would be a mistake to neglect the competition matters in the relationships between the broker and its supply side counterparties.

Interestingly, to date, the primary method used to solve this problem in markets in which the abuse of the leverage of the platform towards its supplier counterparties has been evident, as in the prominent Uber case, has been to reconstruct, in legal terms, the relationship between the platform and the suppliers as a labor law relationship. This has been, for instance, the answer given to this conflict by most of the European scholars, and, with some caveats, this has been the reasoning underlying in the initial case law in

[90] On 7 March 2013 the European Court of Justice of the European Union decided (Case-343/12) that the Belgian prohibition of selling at a loss did not comply with the Unfair Commercial Practices Directive: decision available on the internet at: https://curia.europa.eu/juris/document/document.jsf?docid=135321&doclang=EN (last accessed on 27 September 2021). Similarly, on 19 October 2017, in case C-295/16, the same Court of Justice of the European Union established that the Spanish regulation on sales at a loss is also contrary to EU law: : decision available on the internet at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=195744&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=31609003(last accessed on 27 September 2021).

[91] RODILLA MARTÍ (2021: parts II.2.3 & III).

the United States[92], as well as the core issue settled by the European Court of Justice at the Uber case[93]. This solution, however, fails to solve the problem to its fullest extent. This is not only because there are reasons to conclude that the supposed labor law relationship between Uber and its drivers is, at least, a very special one -which is why some scholars have proposed the creation of a new special legal framework, even within the boundaries of labor law, to regulate this relationship[94]-, but also because it will be complicated to apply this solution to every market in which the digital economy may evolve. For instance, it is hardly convincing to presume that the relationship between Airbnb and the owner of a flat is also a labor law relationship, even when the owner rents the flat on a permanent basis using the platform, as the European Court of Justice lately confirmed[95]. The remedy of considering that the more protective approach of labor law should be applied in order to reduce some of the risks of leverage is only plausible when the relationship between the digital broker and its counterparties is not only profoundly imbalanced, but also more or less permanent, and when the suppliers are producing work, rather than providing goods, for instance… and in a way and with quality standards or an organization of the supply which is clearly decided by the platform. Of course, the problem with categorizing such a relationship as a labor one only increases when the counterpart is a professional or even a company. This is often the case in a bunch of sharing markets that have matured, or in common digital platforms markets, as we see, for instance, in the peer-to-peer accommodation rental market made via Airbnb. In those cases, it is clear that such imbalances between the actors and the protection of some of the counterparties (suppliers) should be granted by a new kind of economic regulation -which should include a broader conception of competition issues- rather than by labor law. As discussed above, the main competition problem posed by digital platforms may

[92] BROWN, Grant E. (2015): "An Uber dilemma: Employees and Independent Contractors in the Sharing Economy" 75 Md. L. Rev. Endnotes.

[93] 20 December 2017 European Court of Justice Decision on Case C-434/15: decision available on the internet at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=198047&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1 (last accessed on 27 September 2021).

[94] TODOLÍ SIGNES, Adrián (2017): "El trabajador en la Uber economy: ni dependiente ni autónomo, sino todo lo contrario", *Trabajo y Derecho. Nueva Revista de Actualidad y Relaciones Laborales*, 25, 2017, pp. 43-60.

[95] 19 December 2019 European Court of Justice Decision on Case C-390/18: decision available on the internet at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=221791&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=31617179 (last accessed on 27 September 2021). See also MURATI, Enzo (2020): "Airbnb and Uber: two sides of the same coin", Media Laws 3/2020, available on the internet at: https://www.medialaws.eu/rivista/airbnb-and-uber-two-sides-of-the-same-coin/ (last accessed on 27 September 2021); POYTON, David (2019): "What makes Uber and Airbnb different in the eyes of the EU -and why it matters", *The Conversation,* available on the internet at: https://theconversation.com/what-makes-uber-and-airbnb-different-in-the-eyes-of-the-eu-and-why-it-matters-121708 (last accessed on 27 September 2021).

be more similar to the risks of a monopsony than to classical monopoly problems. In the current competition regulation, however, the central question is the market power that enables extractive or unfair consumer prices, which is clearly a too timid approach[96].

Finally, some traditional rules or limits in the action of our Competition agencies and bodies are to be widely rethought because this wide leverage of hegemons platforms combines badly with some of the traditional solutions of microeconomic and more economic approach tests. Thus, as it has already been indicated, traditional analysis about acquisitions and mergers that were typically restrictive about when it can be considered a "killer acquisition" will be, without doubts, reshaped to prohibit in the future more of these acquisitions when they may hinder innovation or competition in digital markets, as we already know for sure that they are being used to[97]. Also, as already said, past controversies related to the admissibility of sales at loss, closed as well in America and in Europe with the same conclusion of accepting them as a competitive and positive tool as long as it transfers efficiency to consumers, will be certainly reopened. In both cases, we see how digital platform hegemons use both strategies to difficult or impede competition from new emergent actors, in a way that may not create microeconomic concerns due to the very particular structure of two-sided-markets but that clearly poses macroeconomic risks in terms of cementing a structural dominance of markets that may well hinder competition for years to come, thus freezing the market structure in fields were dynamism, innovation and effective competition are the only guarantees that economic theories about efficiency and its transfer to consumers and society actually happens.

2. Some conclusions about possible changes in the goals and institutional design of competition authorities

The aforementioned problems, as well as the verification that we have not succeeded in solving them with our traditional framework, demonstrates that our competition law must evolve to better confront the risks and challenges posed by the sharing economy. This new approach that our competition authorities must develop should take into

[96] RAHMAN (2015).

[97] CUNNINGHAM, Colleen; EDERER, Florian & MA, Song (2021): "Killer Acquisitions", *Journal of Political Economy*, 129, 3/2021, available on the internet at: https://doi.org/10.1086/712506 (last accessed on 30 September 2021); AFFELDT, Pauline & KESLER, Reinhold (2021): "Big Tech Acquisitions: Towards Empirical Evidence", *Journal of European Competition Law & PracticeI, Vol. 12, 6/2021,* available on the internet at: https://academic.oup.com/jeclap/article/12/6/471/6232342?login=true (last accessed on 30 September 2021); CALVANO, Emilio & POLO, Michele (2021): "Market power, competition and innovation in digital markets: A survey", *Information Economics and Policy*, Vol. 54, available on the internet at: https://www.sciencedirect.com/science/article/pii/S0167624519301994 (last accessed on 30 September 2021).

account not only the micro-economic effects, but also the macro-economic ones. This may boost a trend that is now already emerging, in which the competition authorities coalesce with the market regulators -or even merge, as was the case in the Netherlands and Spain, in both cases in 2013- in order to accomplish this in a coherent way that may allow a better and easier way to introduce macroeconomic analysis and the effects to market structure within competition controls[98]. This trend will accelerate in the coming years, thus forcing a reconsideration of how competition analyses are conducted. In fact, it is noteworthy that the studies that have already been produced by competition bodies in relation to the sharing economy have focused more on the social problems and opportunities posed by it than on strictly competition matters. Nevertheless, they do not seem to realize that by doing so they are changing the nature of its role and beginning a new kind of analysis that will have to be more comprehensive.

The role of law-makers has changed because of technological changes and the increased complexity of our societies. Law does not currently have the capacity to predetermine an ideal solution to any social conflict in a Weberian rationalist way; rather, it must accommodate complex societies in which there is the possibility of finding better solutions ex post because the technological edge in evaluating situations increases every day[99]. In accordance with the reflections above, and in order to encompass this evolution, our competition authorities need to adopt a new approach toward their work that should legitimate their decisions, both from a democratic point of view and from economic efficiency results, in a far better way than the current scheme.

In order to close this work with some *lege ferenda* proposals, we consider that a better understanding of the competitive dynamics and the regulation of the sharing economy specifically, as well as of two-sided markets from a broader perspective, requires administrative bodies that must be designed to analyze competition matters not only from a micro-economic perspective, but also in broader terms (from a macro-economic, but also a social perspective). This is the only way for them to be able to effectively take into account and control the new forms of leverage in that area that are in the hands of the new economic actors. These new forms of leverage may never be used against consumers and may not even affect prices, yet they risk seriously distorting the markets. The procedures should thus be reshaped and replaced by new ones which need to attack these new distortions in a comprehensive way, better founded in economic terms and also more democratically controlled. That will not be enough if there is not a change in

[98] RUIZ PERIS, Juan Ignacio (2012): "La reforma institucional del Derecho de la competencia español", 13-12-2012 *Diario La Ley*.

[99] BOIX PALOP, Andrés (2007): "De McDonalds a Google. La ley ante la tercera revolución productiva", 1 *Teoría y Derecho*, pp. 124-146.

the way the staff is selected, broadening the range of the professionals and areas of expertise beyond that of lawyers and economists. Finally, in order to abandon the "economic only approach" and to integrate an economic and technological analysis into every discretionary decision taken, it would be a good idea to promote a process for the consolidation of competition agencies and market regulation authorities. Because the boundaries between competition and regulation are melting down, the general reshaping of competition control procedures that is needed will produce better results if the capacity for discretionary evaluation given to the authorities includes the ability to compile all the necessary information in the decision process.

This new competition approach in response to the consolidation of the sharing economy and the success of digital brokerage must take legal and economic risks into account within comprehensive analyses and must acknowledge that the effects of technology are far greater than they were previously. It is also essential to integrate the study of other social issues and their effects, as it is essential to do in the regulation of markets. It is not easy to produce such changes. Innovation and experimental regulation may be required until a satisfactory model is reached, particularly because the changes represented by the sharing economy are highly disruptive and innovative[100].

However, to date, our competition authorities have been inconsistent in broadening the scope of their analyses, which can be observed from an examination of the various documents produced so far[101]. They have indeed studied the social and political concerns, but they have done it in an unorganized way, and they have not connected these questions with the competition matters. The European Commission and the various competition bodies in the Member States, to date, have merely considered the platform economy as an opportunity to liberalize markets by loosening some regulations -as the old taxi norms-[102] or as creating favorable circumstances to eliminate traditional bureaucratic burdens -such as those on vacation and tourist rentals[103]-. The fact that the digital economy and their brokerage platforms operates in a sort of "permissionless" environment is generally considered to be positive, fostering innovation and competition by challenging the status quo operators. This is an idea that has received a great deal of

[100] RANCHORDÁS, Sofia (2015): "Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy", 16 *Minn. J.L. Sci. & Tech*, pp. 413-475.

[101] Again, OECD (2010), European Commission (2016), Spanish CNMC (2016), French Rapport (2016).

[102] LEIÑENA MENDIZÁBAL, Elena (2016): "Los nuevos sistemas de utilización compartida de vehículos (carpooling y carsharing): entre la economía colaborativa y la competencia desleal", 296 *Revista de Derecho Mercantil*; BOIX PALOP (2020b).

[103] Cfr. DE LA ENCARNACIÓN VALCÁRCEL (2016), which explains the necessity for new regulations as a result of the success of the rental sharing markets.

attention and deserves more development[104]. Even if this view is accurate, this analysis fails to comprehend the present situation to its fullest extent. A competition comprehensive macro-economic approach that considers all the effects of technology and how to reduce the new brokers' ability to use their power against their counterparties has not yet been developed. This is a sign of how far our competition legal and institutional system still is from being fully adapted to the regulatory necessities of the digital economy and lacks, to the date, the procedures to legitimate its regulation activity in this field not only from a democratic perspective but also in terms of actual economic efficiency.

IV. LIST OF PAPERS AND WORKS MENTIONED IN THIS PAPER

AFFELDT, Pauline & KESLER, Reinhold (2021): "Big Tech Acquisitions: Towards Empirical Evidence", *Journal of European Competition Law & PracticeI, Vol. 12, 6/2021,* available on the internet at: https://academic.oup.com/jeclap/article/12/6/471/6232342?login=true (last accessed on 30 September 2021).

AIGRAIN, Philippe (2012): *Sharing culture and the economy in the Internet age*, Amsterdam, Amsterdam University Press.

ANDERSON, Chris (2006): *The Long Tail: Why the Future of Business Is Selling Less of More,* New York, Hyperion.

ARMSTRONG, Mark (2006): "Competition in two-sided markets", 37-3 *RAND Journal of Economics*, pp. 668-691.

AUTORITÉ DE LA CONCURRENCE & BUNDESKARTELLAMT (2016): *Competition Law and Data.* 10 May 2016. Available on the internet at: http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf (last accessed on 6 October 2020).

BADEN-FULLER, Charles & HAEFLIGER, Stefan (2013): "Business Models and Technological Innovation", 46-6 *Long Range Planning.*

BELK, Russell (2007): "Why not share rather than own?", *The annals of the American Academy of Political and Social Science*, available on the internet at: *http://ann.sagepub.com/content/611/1/126* (last accessed on 27 September 2021).

BERBEZIEUX, Philippe & HERODY, Camille (2016): *Rapport au Premier Ministre sur l'Économie Collaborative,* Paris, La Documentation Française, available on the internet

[104] EDELMAN, Benjamin G. & GERADIN, Damien (2016): "Efficiencies and Regulatory Shortcuts: How Should We Regulate Companies like Airbnb and Uber?", 16-026 *Harvard Business School Working PapersPaper* (2016), available on the internet at: http://ssrn.com/abstract=2658603 (last accessed on 27 September 2021).

at: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/164000100.pdf (last accessed on 1 October 2020).

BOIX PALOP, Andrés (2007): "De McDonalds a Google. La ley ante la tercera revolución productiva", 1 *Teoría y Derecho*.

BOIX PALOP, Andrés, (2017): "La ordenación del transporte urbano colaborativo", Boix, De la Encarnación & Doménech (eds.), *La regulación del transporte colaborativo*, Cizur Menor, Aranzadi - Thomson Reuters, pp. 119-152.

BOIX PALOP, Andrés, (2018): "Estrategias regulatorias para la resolución de los conflictos de intereses generados por la proliferación del alojamiento de corta duración con intermediación digital" in De la Encarnación (dir.) *La regulación del alojamiento colaborativo,* Cizur Menor, Aranzadi - Thomson Reuters, pp. 261-293.

BOIX PALOP, Andrés (2020a): "The Challenges of Urban Mobility and the New Urban Agenda", *Law and the New Urban Agenda,* New York, Routledge.

BOIX PALOP, Andrés (2020b): "Local Leadership and Its Limits in the Deployment of Sustainable Mobility Policies", Finck, Lamping, Moscon & Richter (eds.), *Smart Urban Mobility*, Berlin, Springer, pp. 81-98.

BOTSMAN, Rachel & ROGERS, Roo (2010): *What's mine is yours: the rise of collaborative consumption*, New York, Harpers Collins Publishers.

BROWN, Grant E. (2015): "An Uber dilemma: Employees and Independent Contractors in the Sharing Economy" 75 Md. L. Rev. Endnotes.

BUNDESKARTELLAMT (2010): *Competition in the "New Economy". The Internet, the new driving force,* available on the internet at: http://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/Competition%20in%20the%20New%20Economy.pdf?__blob=publicationFile&v=2 (last accessed on 1 October 2020).

CALVANO, Emilio & POLO, Michele (2021): "Market power, competition and innovation in digital markets: A survey", *Information Economics and Policy*, Vol. 54, available on the internet at: https://www.sciencedirect.com/science/article/pii/S0167624519301994 (last accessed on 30 September 2021).

CARBALLA SMICHOWSKI, Bruno (2016): "Data as a common in the sharing economy: a general policy proposal", *Document de travail du Centre d'Économie de l'Université de Paris Nord CNRS UMR nº 7234*, available on the internet at: https://hal.archives-ouvertes.fr/hal-01386644/document (last accessed on 30 September 2021).

CHEN, Yiwei; HU, Ming & ZHOU, Yun (2019): "Pricing and Matching in the Sharing Economy", Hu (ed.), *Sharing Economy. Making Supply Meet Demand*, Cham Springer, pp. 137-164.

CLEMONS, Eric K. & MADHANI, Nehal (2010): "Regulation of Digital Businesses with Natural Monopolies or Third Party Payment Business Models: Antitrust Lessons from the Analysis of Google", 27-3 *Journal of Management Information Systems*.

CNMC - Comisión Nacional de los Mercados y la Competencia (2016): *Estudio sobre los nuevos modelos de prestación de servicios y la economía colaborativa. Resultados preliminares*, available on the internet at: https://sites.google.com/site/rprelim (last accessed on 1 October 2020).

CUNNINGHAM, Colleen; EDERER, Florian & MA, Song (2021): "Killer Acquisitions", *Journal of Political Economy*, 129, 3/2021, available on the internet at: https://doi.org/10.1086/712506 (last accessed on 30 September 2021).

DE LA ENCARNACIÓN VALCÁRCEL, Ana María (2016): "El alojamiento colaborativo. Viviendas de uso turístico y plataformas virtuales" *5 REALA (Revista de Estudios de la Administración Local y Autonómica),* available on the internet at: <http://revistasonline.inap.es/index.php?journal=REALA&page=article&op=view&path%5B%5D=10350> (last accessed on 1 October 2021).

DE LEON, Ignacio (2016), "Competition Policies in the Internet-based industries: Do we need to reboot the debate?", *Latin American and Caribbean Competition Forum*, available on the internet at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2016)26&docLanguage=En (last accessed on 1 October 2020).

DEMARY, Vera (2015): "Competition in the sharing economy", Paper 19/2015 *Institut der Deutschen Wirtschaft Köln Policy*, available on the internet at: http://scholar.google.es/scholar_url?url=https://www.iwkoeln.de/_storage/asset/235443/storage/master/file/7255909/download/Sharing%2520Economy%2520Policy%2520Paper.pdf&hl=ca&sa=X&scisig=AAGBfm3Wn68Ulcwotmb8GcaKGbJZQgHMgg&nossl=1&oi=scholarr&ved=0ahUKEwj9nsyHhsnOAhWBzxQKHcDOC7sQgAMIICgCMAA (last accessed on 27 September 2020).

DILORENZO, Thomas J. (1996): "The Myth of Natural Monopoly", 9 (2) *The Review of Austrian Economics* (1996), available on the internet at: <https://mises.org/library/myth-natural-monopoly-0> (last accessed on 6 October 2020).

DOMÉNECH PASCUAL, Gabriel (2015): "La regulación de la economía colaborativa (El caso "Uber contra el taxi")", 175-176 *CEFLEGAL*

DUNNE, Niamh (2018): "Competition Law in the Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 104-107.

DYAL-CHAND, Rashmi (2015): "Regulating Sharing: The Sharing Economy as an Alternative Capitalist System", 90-2 *Tulane Law Review*.

ECONOMIDES, Nicholas (1996): "The Economics of Networks", 14 *International Journal of Industrial Organization*.

EDELMAN, Benjamin G. & GERADIN, Damien (2016): "Efficiencies and Regulatory Shortcuts: How Should We Regulate Companies like Airbnb and Uber?", 16-026 *Harvard Business School Working PapersPaper* (2016), available on the internet at: http://ssrn.com/abstract=2658603 (last accessed on 27 September 2021).

EISENMANN, Thomas; PARKER, Geoffrey & VAN ALSTYNE, Marshall W. (2006): "Strategies for Two- Sided Markets", 84-10 *Harvard Business Review* available on the internet at: http://www.hbs.edu/faculty/Pages/item.aspx?num=22459 (last accessed on 6 October 2021).

EUROPEAN COMMISSION (2015): *Consultation on Regulatory environment for platforms, online intermediaries, data and computing and the collaborative industry*. Available on the internet at: https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud (last accessed on 27 September 2020).

EUROPEAN COMMISSION (2016): *A European Agenda for the Collaborative Economy.* Available on internet at: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-356-EN-F1-1.PDF (last accessed on 27 September 2020).

EVANS, David S. & SCHMALENSEE, Richard (2016): *Matchmakers*, Boston, Harvard Business Review Press.

GATA, João E. (2015): "The Sharing Economy, Competition and Regulation", *CPI Europe Column*, available on the internet at: https://www.competitionpolicyinternational.com/the-sharing-economy-competition-and-regulation/ (last accessed on 27 September 2021).

GRAHAM, Mark & ANWAR, Mohammad Amir Niamh (2018): "Two models for a Fairer Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 328-340.

GONZÁLEZ CABRERA, Inmaculada (2020): "Taxis y VTCS/PHVS (*Private Hire Vehicles*) en España en el Reino Unido. Una visión crítica de las regulaciones desarrolladas en las áreas metropolitanas de Barcelona y de Londres", *Revista General de Derecho de los Sectores Regulados*, nº 5.

HUOTARI, Pontus; JÄRVI, Kati; KORTELAINEN, Samuli & HUHTAMÄKI, Jukka (2016): “Winner does not take all: Selective attention and local bias in platform-based markets”, *Technological Forecasting and Social Change*.

LEIÑENA MENDIZÁBAL, Elena (2016): “Los nuevos sistemas de utilización compartida de vehículos (*carpooling* y *carsharing*): entre la economía colaborativa y la competencia desleal”, 296 *Revista de Derecho Mercantil*.

LOBEL, Orly (2016): “The Law of the Platform”, 16-212 San Diego Legal Studies Paper, *Minnesota Law Review*.

MILLER, Stephen R. (2015): “First principles for regulating the sharing economy”, 53 *Harvard Journal of Legislation.*

MITCHELL, Matthew D. & KOOPMAN, Christopher (2018): “Taxis, Taxis and Governance in the Vehicle-For-Hire Industry”, Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 78-90.

MOAZED, Alex & JOHNSON, Nicholas L. (2016): *Modern monopolies. What it takes to dominate the 21st-Century Economy*, New York, St. Martin’s Press.

MONTI, Giorgio (2015): “Competition Law and E-Commerce: Love-hate relationship?”, *European University Institute*, available on the internet at: http://www.jean-monnet-coe.keio.ac.jp/references/giorgio_monti_04.pdf (last accessed on 27 September 2021).

MONTERO, Juan & FINGER, Matthias (2021): *The Rise of the New Network Industries*, New York, Routledge.

MURATI, Enzo (2020): “Airbnb and Uber: two sides of the same coin”, Media Laws 3/2020, available on the internet at: https://www.medialaws.eu/rivista/airbnb-and-uber-two-sides-of-the-same-coin/ (last accessed on 27 September 2021).

NOGUELLOU, Rozen & RENDERS, David,(eds) (2018): *Uber & Taxis. Comparative Law Studies*, Brussels, Bruylant.

OECD (2010): *The economic and social role of Internet intermediaries*, available on the internet at: https://www.oecd.org/internet/ieconomy/44949023.pdf (last accessed on 1 October 2020).

PARKER, Geoffrey G.; VAN ALSTYNE, Marshall W. & CHOUDAR, Sangeet Paul (2016): *Platform Revolution. How networked markets are transformating the economy and how to make them work for you*, New York, Norton & Company.

POSNER, Richard A. (1968): "Natural Monopoly and Its Regulation”, 21 *Stanford Law Review.*

POYTON, David (2019): “What makes Uber and Airbnb different in the eyes of the EU -and why it matters”, *The Conversation,* available on the internet at: https://theconversation.com/what-makes-uber-and-airbnb-different-in-the-eyes-of-the-eu-and-why-it-matters-121708 (last accessed on 27 September 2021).

PROSSER, Tony (2005): *The Limits of Competition Law,* Oxford, Oxford University Press.

RAHMAN, K. Sabeel (2015): *"*Consumer prices are not the only concern raised by dominant companies", 4-05-2015 *Boston Review Forum*, available on the internet at: http://bostonreview.net/forum/k-sabeel-rahman-curbing-new-corporate-power (last accessed on 6 September 2021.

RANCHORDÁS, Sofia (2015): "Innovation experimentalism in the age of the sharing economy", 19:4 *Lewis & Clark Law Review*.

RANCHORDÁS, Sofia (2015): "Does Sharing Mean Caring? Regulating Innovation in the Sharing Economy", 16 *Minn. J.L. Sci. & Tech*,

RIFKIN, Jeremy (2014): *Zero marginal cost society. The Internet of things, the collaborative commons, and the eclipse of capitalism,* New York, St. Martin's Press.

RIORDAN, Michael H. (1992): "Regulation and preemptive technology adoption", 23-3 *The RAND Journal of Economics*.

ROCHET, Jean-Charles & TIROLE, Jean (2003): "Platform Competition in Two-Sided Markets", 1-4 *Journal of the European Economic Association*.

ROCHET, Jean-Charles & TIROLE, Jean (2006): "Two-Sided Markets: A progress report", 37-3 *The RAND Journal of Economics,* pp. 645-667, available on the internet at: https://www.jstor.org/stable/25046265?seq=1#page_scan_tab_contents (last accessed on 1 October 2020).

RODILLA MARTÍ, Carmen (2018): *Los Precios Excesivos por Explotación como Ilícito del Derecho de la Competencia*, Cizur Menor, Aranzadi - Thomson Reuters.

RODILLA MARTÍ, Carmen (2021): "Los mercados de plataformas digitales: entre el Derecho de la Competencia y la Regulación", *Revista General de Derecho de los Sectores Regulados*, nº 8.

RUIZ PERIS, Juan Ignacio (2012): "La reforma institucional del Derecho de la competencia español", 13-12-2012 *Diario La Ley*.

SCHMIDTCHEN, Dieter; ALBERT, Max & VOIGT, Stefan (2007): "The More Economic Approach to European Competition Law", 24 Conferences ion new Political Economy*,* Tübingen*,* Mohr Siebeck;

SCHOENBAUM, Naomi (2018): "Intimacy and Equality in the Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 459-470.

SCHWEITZER, Heike & PATEL, Kiran Klaus (2013):, "EU Competition Law in Historical Context: Continuity and Change", Patel and Schweitzer (eds.), *The Historical Foundations of EU Competition Law*, Oxford, Oxford University Press, 2013.

SORIANO ARNANZ, Alba (2021a): *Data protection for the prevention of algorithmic discrimination. Protecting from discrimination and other harms caused by algorithms through privacy in the EU and US: possibilities shortcomings and proposals*, Cizur Menor, Aranzadi-Thomson Reuters.

SORIANO ARNANZ, Alba (2021b): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, nº 56.

SORIANO ARNANZ, Alba (2021c): "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Teoría y Método. Revista de Derecho Público*, Vol. 3(2021) available on the internet at: https://doi.org/10.37417/RPD/vol_3_2021_535 (last accessed on 30 October 2021).

SORIANO ARNANZ, Alba (2021d): "La propuesta de reglamento de inteligencia artificial de la UE y los sistemas de alto riesgo", *Revista General de Derecho de los Sectores Regulados*, nº 8.

SRINAGESH, Padmanabhan (1998): "Internet Cost Structures and Interconnection Agreements", McKnight and Bailey (eds.), *Internet Economics*, Cambridge, The MIT Press.

THÉPOT, Florence (2012): "Market Power in Online Search and Social Networking: a Matter of Two-Sided Markets", *4/2012 CLES Working Paper Series University College London* (2012), available on the internet at: <http://www.ssrn.com/abstract=2307009> (last accessed on 1 October 2020).

TODOLÍ SIGNES, Adrián (2017): "El trabajador en la Uber economy: ni dependiente ni autónomo, sino todo lo contrario", *Trabajo y Derecho. Nueva Revista de Actualidad y Relaciones Laborales*, 25, 2017, pp. 43-60.

UNITED KINGDOM COMPETITION EXPERT PANEL (2019): Unlocking digital competition, available on the internet at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf (last accessed on 20 October 2021).

VALLAS, Steven & SCHOR, Juliet B. (2020): "What Do Platforms Do? Understanding the Gig Economy", Annual Review of Sociology, 46, pp. 273-294, available on the internet at: https://doi.org/10.1146/annurev-soc-121919-054857 (last accessed on 1 October 2021).

WEYL, E. Glen (2010): "A Price Theory of Multi-sided Platforms", 100(4): *American Economic Review.*

WIGGER, Angela (2008): *Competition for competitiveness: The Politics of the Transformation of the EU Competition Regime*, doctoral thesis available on the internet at: <http://dare.ubvu.vu.nl/handle/1871/15601> (last accessed on 1 October 2020).

WOLF, Dieter (1999) "La réforme des services publics en Allemagne", Jean-Marie Chevalier and Ivar Ekeland and Marie-Anne Frison-Roche (eds.), *L'idee de service public est-elle encore soutenable?*, Paris, P.U.F., pp. 11-20.

WOSSKOW, Debbie (2015): *Unlocking the sharing economy. An independent review. Report to UK Business Minister,* 2015, available on the internet at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378291/bis-14-1227-unlocking-the-sharing-economy-an-independent-review.pdf> (last accessed on 1 October 2021).

ZALE, Kellen (2018): "Scale and the Sharing Economy", Davidson, Finck & Infranca (eds.), *The Law of the Sharing Economy;* Cambridge, Cambridge University Press, pp. 38-50.

ZURIMENDI ISLA, Aitor (2020): "Naturaleza jurídica de las plataformas digitales", *Revista General de Derecho de los Sectores Regulados*, nº 6.

UNA APROXIMACIÓN AL RÉGIMEN JURÍDICO DE LOS SERVICIOS DIGITALES: ESTRUCTURA Y SISTEMÁTICA DEL MARCO JURÍDICO DE LOS SERVICIOS PRESTADOS EN LÍNEA

Por

JOSÉ VIDA FERNÁNDEZ [1]
Profesor Titular de Derecho Administrativa
Universidad Carlos III de Madrid

jose.vida@uc3m.es

Revista General de Derecho de los Sectores Regulados 8 (2021)

RESUMEN: Los servicios que se prestan en entornos digitales están siendo objeto de una creciente regulación a nivel europeo. Se trata de normas que van sumándose para conformar el marco jurídico de estos servicios prestados en línea a través de Internet. Sin embargo, resulta difícil identificar la estructura de este marco jurídico ya que estas normas no han sido elaboradas de forma coordinada ni responden a un plan conjunto que permita estructurarlas de forma ordenada. Se hace necesario así identificar y sistematizar toda esta normativa para así poder determinar el régimen jurídico aplicable a cada uno de estos servicios dentro del entorno digital.

PALABRAS CLAVE: Sector digital, servicios de sociedad de la información, servicios digitales, servicios en línea, plataformas digitales, servicios de telecomunicaciones, servicios audiovisuales, servicios OTT.

SUMARIO: I. El problema de la determinación del régimen jurídico aplicable a los servicios digitales. II. La normativa horizontal básica de los servicios prestados en el entorno digital: El régimen jurídico de los servicios de la sociedad de la información. 1. Origen de la definición de los servicios de la sociedad de la información: Directiva 98/34/CE; 2. El marco normativo básico los servicios de la sociedad de la información: Directiva 2000/31/CE. III. La nueva normativa horizontal de los principales servicios prestados en el entorno digital: El régimen de los servicios intermediarios (servicios digitales). 1. El problema de la identificación de los servicios digitales. 2. La nueva regulación de los servicios intermediarios: Propuesta de Ley de Servicios Digitales. IV. Normas específicas sobre determinados aspectos de los servicios prestados en el entorno digital: Contratación de servicios digitales, servicios de intermediación para profesionales y servicios de plataformas básicas. 1. La contratación de contenidos y servicios digitales: Directiva (UE) 2019/770. 2 Los servicios de intermediación en línea para usuarios profesionales: Reglamento (UE) 2019/1150. 3. Los servicios de plataformas básicas: Propuesta de Ley de Mercados Digitales. V. La normativa sectorial aplicable a determinados servicios prestados en el entorno digital. 1. El desarrollo de servicios digitales que desborda los regímenes jurídicos sectoriales: Servicios over the top (OTT) y el problema del playing level field. 2. Servicios digitales que son servicios de comunicaciones

[1] El presente trabajo se ha realizado como parte del proyecto de investigación “El impacto de la inteligencia artificial en los servicios públicos: Un análisis jurídico de su alcance y consecuencias en la asistencia sanitaria” (PGC2018-098243-B-I00) que se desarrolla bajo la dirección del profesor José Vida Fernández dentro de la convocatoria 2018 de «Proyectos de I+D de Generación de Conocimiento» del Programa Estatal de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+i del Ministerio de Ciencia e Innovación.

electrónicas: Directiva (UE) 2018/1808, de Código Europeo de Comunicaciones Electrónicas. 3. Servicios de comunicación audiovisual: Directiva (UE) 2018/1808 de servicios de comunicación audiovisual. 4. Servicios digitales de intermediación que son parte integrante de otros servicios sometidos a normas sectoriales (servicios de alojamiento, transporte y otros). VI. Conclusiones. VII. Bibliografía.

ABSTRACT: Services provided in digital environments are increasingly being regulated in the European Union. Different acts and regulations are adopted and constitute the legal framework for the Internet online services. However, it is difficult to identify the structure of this legal framework as these rules have not been adopted jointly and do not follow a plan that would allow to sort them. It is therefore necessary to identify and systematize all these acts and regulations in order to determine the legal regime applicable to each of these digital services.

KEYWORDS: Digital sector, information society services, digital services, online services, digital platforms, telecommunications services, audiovisual services.

I. EL PROBLEMA DE LA DETERMINACIÓN DEL RÉGIMEN JURÍDICO APLICABLE A LOS SERVICIOS DIGITALES

El tránsito a una realidad digital en línea no ha venido acompañado de una regulación global, sistemática y acabada de este nuevo contexto. Este fenómeno no es (sólo) consecuencia del desfase estructural que sufre el Derecho con respecto a los cambios socio-económicos –que se acentúa cuando se trata innovaciones tecnológicas–, sino que se debe a la imposibilidad de abarcar en un régimen jurídico único y homogéneo todas las manifestaciones del nuevo entorno digital[2].

En este sentido las actividades y servicios desarrollados en línea y que se pueden identificar genéricamente como servicios digitales –por más que no existan como categoría legal– no se encuentran sometidos a un régimen jurídico único, sino que, en función de sus características quedan sometidos a diferentes normativas en cuanto servicios de la sociedad de la información –que pueden estar a su vez sometidos a medidas específicas en cuanto servicios intermediarios, guardianes de acceso, etc.– pero, también, pueden ser calificados como otro tipo de servicios –de telecomunicaciones, audiovisuales, transportes, alojamiento, etc.– y quedar sometidos a todo un régimen diferenciado de carácter especial.

De este modo, los servicios digitales, en cuanto categoría que se utiliza aquí de forma convencional para identificar a los servicios prestado en línea a través de Internet, se ven sometidos a una multiplicidad de regímenes jurídicos que coexisten solapados y

[2] Los problemas estructurales de la regulación de las actividades desarrolladas en línea a través de Internet fueron identificados de forma temprana por Santiago MUÑOZ MACHADO (2000) y más recientemente se hace eco de esta cuestión Moisés BARRIO ANDRÉS (2020: 147 a 167).

yuxtapuestos, tal y como ocurre en el entorno analógico, sin que la realidad digital haya quedado sometida a un régimen jurídico uniforme. Esto es así tanto por lo que respecta a la Unión Europea, como para el resto de ordenamientos jurídicos ya que resulta inevitable disponer regímenes jurídicos específicos para las distintas actividades y servicios que se prestan en línea en función de su naturaleza específica.

A partir de esta constatación surgen las dificultades para determinar el régimen jurídico aplicable en cada caso a los servicios digitales ya que se han ido incrementando las normas que les afectan, sin que éstas se hayan adoptado de forma conjunta y ordenada, y sin que cada éstas ofrezcan unos criterios claros y definitivos que permitan concretar su aplicación. Esta circunstancia se aprecia en la distinta clasificación de estos servicios digitales entre los que se puede distinguir servicios de la sociedad de la información, servicios intermediarios, servicios de plataformas básicas, además de servicios de comunicaciones electrónicas, servicios audiovisuales y otros servicios que también se prestan en línea a través de Internet.

Este trabajo trata de aportar algo de luz sobre esta cuestión al ofrecer una visión panorámica y ordenada del marco normativo que la Unión Europea ha dispuesto para todos estos servicios, tratando de sistematizar y concretar el régimen jurídico aplicable a los distintos servicios digitales en atención a sus características. Debe tenerse en cuenta que la finalidad del trabajo no es el análisis detallado del contenido del marco jurídico aplicable a los servicios digitales a nivel europeo o nacional, sino que se limita a identificar su estructura y sistemática para concretar la normativa a la que quedan sometidos cada uno de estos servicios.

Este recorrido por la normativa aplicable a los servicios digitales a nivel europeo se lleva a cabo conforme a un criterio sistemático, a partir de la estructura en que quedan dispuestas las distintas normas que responde al siguiente esquema:

a) Una normativa horizontal de contenido mínimo que se recoge en el régimen de los servicios de la sociedad de la información (apartado 2).

b) Unas nuevas normas horizontales de intervención ex ante que lo completan por lo que se refiere a los servicios intermediarios o servicios digitales (apartado 3)

c) Unas normas específicas sobre ciertos aspectos de los servicios de la sociedad de la información: Contratación de servicios digitales, servicios de intermediación para profesionales y servicios de plataformas básicas (apartado 4)

d) Unas normas verticales de carácter especial que desplazan a la normativa horizontal: Servicios de comunicaciones electrónicas, servicios de comunicación audiovisual y otros servicios sectoriales (apartado 5).

Quedan al margen las normas transversales que pueden afectar a dimensiones concretas de los servicios digitales y forman parte del marco jurídico que les resulta aplicable, pero que no tienen como finalidad y objeto específicos regular de manera explícita y determinada estos servicios. Se trata de todas aquellas normas que inciden sobre los servicios digitales, pero no los tienen por objeto, como es el caso de la normativa sobre protección de datos personales, sobre ciberseguridad, sobre protección de consumidores, salud pública, defensa de la competencia, propiedad intelectual, entre otras.

Como se puede comprobar, el régimen jurídico de los servicios prestados en un entorno digital es un verdadero puzle compuesto por normas que no se ajustan perfectamente entre ellas ya que se han ido dictando de forma desordenada y sin responder a un planteamiento común que tuviese en cuenta el marco jurídico resultante. A través de este trabajo se trata de identificar y sistematizar las distintas normas que componen este complejo marco jurídico para tratar dotarlo de estructura y así facilitar la determinación del régimen jurídico de cada de los distintos servicios digitales que se prestan en línea.

II. LA NORMATIVA HORIZONTAL BÁSICA DE LOS SERVICIOS PRESTADOS EN EL ENTORNO DIGITAL: EL RÉGIMEN JURÍDICO DE LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

1. Origen de la definición de los servicios de la sociedad de la información: Directiva 98/34/CE

Dentro del creciente número de normas aplicables a los servicios que se prestan en línea en el entorno digital se puede identificar un bloque normativo que se proyecta de forma transversal y que constituye un verdadero régimen jurídico común que se aplica por defecto a todos ellos en cuanto servicios de la sociedad de la información junto a normas adicionales para algunas categorías de estos servicios (servicios intermediarios constituidos por grandes plataformas). Por lo tanto, esta normativa sobre los servicios de la sociedad de la información actúa como un verdadero bajo continuo que está presente en la prestación de todos los servicios digitales, y solamente resulta desplazada de forma puntual por normas especiales sectoriales cuando responden a las características de otro tipo de servicios como las telecomunicaciones, los audiovisuales, los financieros, de transporte, de alojamiento, etc.

A nivel europeo, la regulación de los servicios prestados en línea se inició a finales de la década de los años noventa del siglo pasado con una normativa dirigida a la supervisión de las normativas nacionales que se estaban empezando a dictar para regular el creciente número de actividades desarrolladas a través de un incipiente Internet, y que se contenía

en la Directiva 98/34/CE sobre reglas relativas a los servicios de la sociedad de la información[3].

En efecto, con esta primera iniciativa se estableció un mecanismo de control de las medidas adoptadas por los Estados sobre las actividades en línea obligándoles a informar de las mismas para poder así actuar al respecto. Con esta finalidad se introdujo el concepto de "servicios de la sociedad de la información" cuya definición va a servir en adelante para fijar el ámbito de aplicación de las normas destinadas a los servicios prestados en línea que se van a ir multiplicando y sofisticando con el desarrollo de Internet.

Estos "servicios de la sociedad de la información" son los que se denominan comúnmente como servicios en línea, servicios prestados a través de Internet o, genéricamente, servicios digitales. Como puede comprobarse la expresión original que se emplea para denominarlos es muy propia de una época en la que se hablada de la "era del conocimiento y de la información" en términos económicos y sociológicos, si bien ha quedado algo desfasada en la actualidad. De hecho, en el ámbito de la Unión Europea, se está desplazando el término de servicios de la sociedad de la información por el de servicios digitales, que se utilizan de una forma algo confusa a pesar de que se ha incorporado a la normativa reguladora de estos servicios, como se podrá comprobar más adelante.

Desde su introducción en esta normativa, la definición de los servicios de la sociedad de la información se ha mantenido sin modificaciones como aquellos servicios prestados normalmente a título oneroso[4] a distancia[5], por vía electrónica[6], y a petición individual de

[3] Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, que resultó profundamente modificada por la Directiva 98/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso.

[4] Se trata, por tanto, de servicios a cambio de una remuneración, sea directa o indirecta.

[5] Sin que las partes estén presentes simultáneamente. De hecho, el Anexo I indica que no pueden considerarse servicios prestados a distancia aquellos prestados en presencia física del prestador y del destinatario, aunque impliquen la utilización de dispositivos electrónicos (como una revisión médica con aparatos electrónicos, la consulta de un catálogo electrónico, la reserva de un billete en una red de ordenadores, o juegos de un salón recreativo, siempre que se concurra la presencia física del cliente).

[6] Es decir, mediante un equipo electrónico para el tratamiento y el almacenamiento de datos. Igualmente, en el Anexo I hace una enumeración servicios que se consideran como no ofrecidos «por vía electrónica», como son aquellos cuyo contenido es material aunque se presten utilizando dispositivos electrónicos (expendeduría de dinero por cajeros o de billetes de tren, acceso a redes de carretera, aparcamientos, etc.), servicios fuera de línea (distribución de soportes con programas informáticos en disquetes), servicios no prestados por medio de sistemas electrónicos de tratamiento o almacenamiento de datos (servicios de telefonía vocal, de fax y télex); servicios prestados por medio de telefonía vocal o fax (consulta médica, jurídica, marketing).

un destinatario de servicios[7], requisitos que deben cumplirse con carácter acumulativo, tal y como se contiene en el artículo 1.2 y en el Anexo I de la Directiva 98/34/CE y de la Directiva (UE) 2015/1535 [8] (que la sustituye) y se recoge en la normativa interna de los Estados Miembros[9].

Como se ha indicado, esta es la primera normativa a nivel europeo sobre esa nueva realidad que eran los servicios en línea digitales prestados a través de Internet, que no contenía ninguna medida de contenido prescriptivo positivo y se limitó a establecer un sistema de información para supervisar y controlar la regulación de los Estados en este ámbito, que actualmente se recoge en la Directiva (UE) 2015/1535 y que se mantiene en términos muy similares a los originales.

Resulta significativo, sin embargo, que en esta primera normativa que apenas tenía contenido se plantease ya la problemática del ámbito de aplicación y se tuviese que llevar a cabo una definición tan detallada de los servicios de la sociedad de la información, y también se procediese a una detallada distinción con respecto a otros servicios como son los audiovisuales (art. 1.2 in fine), las telecomunicaciones, los financieros y los mercados de valores (art. 1.5).

2. El marco normativo básico los servicios de la sociedad de la información: Directiva 2000/31/CE

El verdadero punto de partida de la normativa europea en materia de servicios de sociedad de la información fue la Directiva 2000/31/CE sobre el comercio electrónico[10], ya que es la que dispone un régimen jurídico específico para este tipo de servicios, más allá del sistema de vigilancia establecido por la normativa precedente que introdujo la definición de estos servicios.

En efecto, la Directiva 2000/31/CE se aprobó con el objetivo de suprimir los obstáculos a la prestación de actividades económica en línea coordinando las legislaciones

[7] Con respecto a la transmisión de datos a petición individual, el Anexo I también enumera servicios que no son prestados a petición individual como son los de transmisión de datos sin petición individual y destinados a la recepción simultánea por un número ilimitado de destinatarios (transmisión punto o multipunto) entre los que se encuentran los servicios de radiodifusión televisiva, sonora o teletexto, en su versión por ondas hertzianas.

[8] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

[9] En el caso de España, en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), apartado a) del Anexo.

[10] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

nacionales y aclarando conceptos para un mejor funcionamiento del mercado interior. Con este objetivo se dispone un marco jurídico necesario para garantizar la libre circulación de los servicios de la sociedad de la información entre Estados miembros.

Es decir, se trata de una regulación de mínimos que no pretende ordenar el mercado de servicios de sociedad de la información –como veremos que se busca en las propuestas de reglamentos sobre los servicios y plataformas digitales en tramitación– ni armonizar las legislaciones nacionales sino que se limita a coordinarlas para garantizar que la prestación de estos servicios se haga con un alto nivel de protección de los objetivos de interés general y, en especial, del consumidor, salud pública, menores, etc.

Por lo tanto, este régimen jurídico básico de los servicios de la sociedad de la información parte del libre desarrollo de la prestación de estos servicios con respecto a los que no se le puede exigir ningún título habilitante (principio de no autorización previa) y simplemente se imponen unas obligaciones genéricas (de identificación del prestador, información, etc.) para facilitar el ejercicio de los derechos de los usuarios, a la vez que se concretan una serie de responsabilidades para garantizar la protección de dichos derechos.

En cuanto al ámbito de aplicación de la Directiva 2000/31/CE viene determinado por la definición que se hace en la misma de los servicios de la sociedad de la información –que es la que se recoge de la Directiva 98/34/CE, a la que se remite el artículo 2 a)–, si bien se lleva a cabo de forma mucho más precisa para determinar su ámbito de aplicación, ya que van apareciendo una amplia variedad de actividades económicas que se desarrollan en línea.

Así, con respecto al carácter oneroso de estos servicios, nada impide que se incluyan servicios no remunerados por sus destinatarios, como ofrecer información en línea o comunicaciones comerciales, o los que ofrecen instrumentos de búsqueda, acceso y recopilación de dato, en la medida que pueden entenderse remunerados por otros que no sus destinatarios (anunciantes, etc.).

En cuanto a la prestación a distancia de los servicios, cuando se trata del comercio electrónico (venta en línea), no incluye las actividades complementarias como la entrega de mercancías en sí misma o la prestación de servicios fuera de la línea. Sin embargo, la exclusión de actividades que, por su naturaleza, no pueden realizarse a distancia ni por medios electrónicos se va reduciendo de forma drástica conforme se va extendiendo el proceso de digitalización, ya que actividades como el control legal de la contabilidad de las empresas o el reconocimiento médico que se consideraban entonces presenciales pueden llevarse a cabo ahora a distancia con igual precisión.

Por lo que se refiere a la prestación por vía electrónica, y a petición individual de un destinatario la definición de los servicios de sociedad de la información se vuelve más

compleja. Por una parte, se indica que quedan cubiertos los servicios consistentes en transmitir información a través de una red de comunicación, o albergar información facilitada por el destinatario del servicio; pero quedan fuera los servicios de radiodifusión sonora (radio) o televisiva (televisión analógico o digital) en tanto no se prestan a petición individual, aunque si quedarían incluidos servicios como el vídeo a la carta o el envío de comunicaciones comerciales por correo electrónico ya que se transmiten entre dos puntos[11].

Como puede comprobarse, se trata de una definición legal de los servicios de la sociedad de la información de carácter flexible y expansiva que abarca una enorme cantidad y variedad de servicios en constante transformación, en las que se incluyen tanto servicios que ofrecen funcionalidades de forma directa y final a los usuarios, como servicios de intermediación que facilitan el acceso a otros servicios o a contenidos e información (transmisión de datos, copia temporal de páginas o alojamiento de información en servidores).

Para contener el carácter expansivo de esta definición, el ámbito de aplicación de la Directiva 2000/31/CE también queda delimitado mediante la exclusión de determinadas actividades como las propias de los notarios o profesiones equivalentes que implican el ejercicio de la autoridad pública, el ejercicio de la abogacía y las actividades de juegos de azar que impliquen apuestas de valor monetario incluidas loterías y apuestas (art. 1.5 d).

Resulta llamativo que, a diferencia de la Directiva 98/34/CE, no se lleve a cabo una exclusión de determinados servicios sometidos a un régimen específico como las telecomunicaciones, los audiovisuales, los financieros o los mercados de valores porque precisamente el criterio es distinto. Lo que se pretende en la Directiva 2000/31/CE es una aplicación generalizada a todos los servicios que cumplan con la definición de los servicios de sociedad de la información, sin perjuicio de que estos servicios queden sometidos a una normativa específica, constituyendo así de forma agregada un marco jurídico para la provisión en línea de dichos servicios[12].

Por lo demás, el resto de normas que enmarca las actividades desarrolladas a través de servicios de la sociedad de la información se sigue aplicando normalmente sin perjuicio

[11] El uso del correo electrónico o, por ejemplo, de sistemas equivalentes de comunicación entre individuos, por parte de personas físicas que actúan fuera de su profesión, negocio o actividad profesional, incluso cuando los usan para celebrar contratos entre sí, no constituyen un servicio de la sociedad de la información.

[12] Así puede comprobarse cuando se refiere a los servicios financieros, al señalar que la Directiva 2000/31/CE, junto con la Directiva sobre comercialización a distancia de servicios financieros destinados a los consumidores, contribuye a la creación de un marco jurídico para la provisión en línea de servicios financieros, sin que impida futuras iniciativas en el campo de los servicios financieros, en particular en relación con la armonización de normas de conducta en este terreno (considerando 27).

del régimen de éstos contenido en la Directiva 2000/31/CE que indica específicamente que la normativa sobre consumidores, salud, seguridad de los productos, publicidad, etc. para confirmar que dicha normativa se seguirá aplicando en su integridad a los servicios de la sociedad de la información (considerandos 11 y 21). Por si hubiera alguna duda, se aclara así que el prestar servicios en línea no permite hacer tabula rasa de todo el ordenamiento, por lo que el régimen de los servicios de la sociedad de la información no puede considerarse como un régimen ni exclusivo ni excluyente del resto de la normativa.

III. LA NUEVA NORMATIVA HORIZONTAL DE LOS PRINCIPALES SERVICIOS PRESTADOS EN EL ENTORNO DIGITAL: EL RÉGIMEN DE LOS SERVICIOS INTERMEDIARIOS (SERVICIOS DIGITALES)

1. El problema de la identificación de los servicios digitales

Durante las últimas dos décadas se ha producido un incremento extraordinario de los servicios de la sociedad de la información que se han multiplicado y perfeccionado, ofreciendo cada vez más funcionalidades que son utilizadas de forma continua y relevante en la vida diaria por millones de usuarios. El crecimiento y transformación de estos servicios ha dado lugar a que estén transformando todos los sectores económicos, ya sea porque son capaces de sustituir servicios prestados por otros medios (como ha ocurrido con los servicios de telecomunicaciones –mensajería instantánea– o con los audiovisuales –plataformas de video bajo demanda–) o porque alteran o, incluso, absorben el funcionamiento del mercado como intermediarios (plataformas de transporte o alojamiento).

Este proceso de maduración y desarrollo ha coincidido con un cambio en su denominación en los últimos años ya que, como se ha adelantado, se ha ido abandonando su tradicional referencia a los servicios de la sociedad de información que ha sido sustituida a nivel por la de servicios digitales, aunque de una forma muy confusa por parte de las instituciones de la Unión.

Por una parte, se ha utilizado el término “servicios digitales” como sinónimo de los servicios de la sociedad de la información, como puede comprobarse en la normativa europea sobre ciberseguridad, como es la Directiva (UE) 2016/1148 de seguridad de las redes y sistemas de información (Directiva NIS[13]), ya que se habla de los proveedores de servicios digitales como unos de los obligados a cumplir los requisitos en materia de

[13] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

seguridad y notificación de incidentes, identificando los servicios digitales como servicios de la sociedad de la información[14].

Asimismo, en la Propuesta de Reglamento de la Ley de servicios digitales[15], se utiliza esta expresión como equivalente a los servicios de la sociedad de la información, aunque en realidad no es así, ya que los servicios digitales que la misma regula no abarca a la totalidad de aquellos. En efecto, la propuesta de Ley de servicios digitales no los define y se centra en los servicios de sociedad de la información intermediarios (de mera transmisión, de memoria tampón o de alojamiento de datos).

Pero es que incluso, la propia Unión Europa ha dictado una Directiva (UE) 2019/770 sobre contratos de suministro de contenidos y servicios digitales [16], cuya definición no tiene nada que ver con la de los servicios de la sociedad de la información, aunque pueda coincidir sustancialmente con estos, como veremos más adelante.

En definitiva, y como puede comprobarse, no existe una definición clara de lo que son los servicios digitales, aunque pueden equipararse a los servicios de la sociedad de la información, tal y como se hace en la Propuesta de Reglamento de la Ley de servicios digitales y en diversos documentos de la Unión Europea, como denominación genérica de los servicios prestados en línea a través de Internet.

2. La nueva regulación de los servicios intermediarios: Propuesta de Ley de Servicios Digitales

Más allá de las cuestiones terminológicas, lo que resulta evidente es que el marco jurídico de los servicios prestados en el entorno digital se ha ido ampliado e intensificando conforme se han ido extendiendo y desarrollando dichos servicios.

En efecto, la normativa horizontal aplicable a los servicios de la sociedad información contenida en la Directiva 2000/31/CE ha resistido durante más de dos décadas gracias a que tiene un contenido de mínimos que ha permitido el libre desarrollo de estos servicios. Sin embargo, trascurridos veinte años desde aprobación, se ha comprobado que no se puede seguir manteniendo un régimen tan elemental ya que la evolución del entorno digital y de las actividades económicas que se desarrollan en el mismo exige una intervención más intensa que garantice el buen funcionamiento del mercado y cree un entorno en línea

[14] El artículo 4.5 define los servicios digitales por remisión a la definición de los servicios de sociedad de la información de la Directiva (UE) 2015/1535.

[15] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE, presentada el 15.12.2020 COM(2020) 825 final.

[16] Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.

más seguro, predecible y confiable, en particular por lo que se refiere a determinados actores como son las grandes plataformas digitales[17].

Se plantea así la propuesta de Reglamento de Ley de Servicios Digitales como una normativa horizontal con la que se viene a completar el régimen de determinados servicios de la sociedad de la información que ya están contenidos en la Directiva 2000/31/CE, en concreto de los prestadores de servicios intermediarios –especialmente las plataformas en línea como los mercados y las redes sociales–, y para los que se establece un marco horizontal específico que sustituye al contenido en la sección 4ª del Capítulo II de dicha norma por razón del crecimiento exponencial que ha experimentado el uso que se hace de dichos servicios (considerando 6 y artículo 2 f) de la Propuesta de Ley de Servicios Digitales).

Por lo tanto, la propuesta de Ley de Servicios Digitales no se aplica a la totalidad de los servicios de la sociedad de la información sino a los servicios intermediarios, que ya habían sido clasificados en la Directiva 2000/31/CE en servicios como de mera transmisión, de memoria tampón y de alojamiento de datos[18]. A partir de este objeto, el contenido de la propuesta de la Ley de Servicios Digitales dispone un conjunto de obligaciones básico a los que se van añadiendo otras obligaciones adicionales en función de la relevancia de estos servicios intermediarios que los clasifica como una matrioska o muñeca rusa. Así, dentro de los servicios intermediarios distingue los servicios de alojamiento que incluye otras subcategorías como son los servicios en la nube o los servicios de alojamiento web, para los que prevé obligaciones adicionales específicas. Dentro de esta subcategoría de servicios de alojamiento web se encuentran las plataformas en línea que van desde las redes sociales, a los medados en línea o las plataformas de mercado colaborativo. Y dentro de estas plataformas en línea distingue una categoría de plataformas en línea de muy gran tamaño que son aquellas que superan los cuarenta y cinco millones de destinatarios (un 10 % de la población de la Unión) para las que añade unas obligaciones más por razón de su impacto que se suman a todas las anteriores.

Por lo tanto, se trata de una norma de geometría variable que se aplica genéricamente a los servicios intermediarios pero que prevé un contenido distinto en función del tipo de

---

[17] Sobre los desafíos que plantean las plataformas desde una perspectiva jurídica vid. Teresa RODRÍGUEZ DE LAS HERAS (2020)

[18] El servicio de mera transmisión consiste en transmitir, en una red de comunicaciones, información facilitada por el destinatario del servicio o en facilitar acceso a una red de comunicaciones; el servicio de memoria tampón (caching) consiste en transmitir por una red de comunicaciones información facilitada por el destinatario del servicio, que conlleve el almacenamiento automático, provisional y temporal de esta información, con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de estos; y el servicio de «alojamiento de datos» consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este (art. 2 f) Propuesta de Ley de Servicios Digitales). Vid José Juan CASTELLÓ PASTOR (2021).

que se trate sobre un esquema de obligaciones acumulativas que se van intensificando en función de la naturaleza de los riesgos sociales que representan sus servicios según se trata de servicios de alojamiento de datos, y, dentro de estos, de plataformas en línea; y, dentro de estos, plataformas en línea de muy gran tamaño[19]. Asimismo, se actualizan, aclaran y armonizan para estos servicios intermediarios las normas de responsabilidad para los prestadores de servicios intermediarios, que pasan de la Directiva 2000/31/CE a esta nueva Ley de Servicios Digitales incorporando la jurisprudencia recaída al respecto. Todo esto se completa con unos mecanismos de cooperación y coordinación para la supervisión de las obligaciones y ejecuten la nueva normativa por parte de los Estados Miembros.

En todo caso debe tenerse en cuenta que la propuesta de Reglamento de Ley de Servicios Digitales no contiene el marco jurídico global de los servicios digitales como reza en su título ya que, como se ha indicado, ni siquiera se llegan a definir, sino que dispone un régimen específico para los servicios intermediarios que son los más numerosos dentro de los servicios de la sociedad de la información, que sigue siendo la categoría matriz. Esto explica que el ámbito de aplicación de esta propuesta de Reglamento de Ley de Servicios Digitales se haga depender de la definición de los servicios de sociedad de la información y de los servicios intermediarios contenida en la Directiva 2000/31/CE.

De este modo, y al igual que sucede con la Directiva 2000/31/CE, el régimen que contiene esta propuesta Reglamento de Ley de Servicios Digitales cede frente a regímenes especiales de determinados servicios intermediarios que se someten a regímenes especiales como son los servicios de telecomunicaciones, audiovisual, transporte o alojamiento. Esta normativa especial se aplicará con carácter preferente y

[19] Las obligaciones acumulativas previstas en la propuesta de reglamento de Ley de Servicios Digitales se estructuran de la siguiente forma:

- Se parte de los servicios de intermediación en general sometidas a unas obligaciones básicas como son la elaboración de informes de transparencia; fijación de requisitos sobre las condiciones de servicio, habida cuenta de los derechos fundamentales; la cooperación con las administraciones nacionales con arreglo a órdenes; y contar con puntos de contacto y, en su caso, representante legal.
- En el caso de los servicios intermediarios de alojamiento de datos se suma a éstas la obligación de notificación y adopción de medidas y obligación de informar a los usuarios.
- Para los servicios intermediarios de alojamiento de datos que sean plataformas en línea, se añade a lo anterior, el contar con mecanismos de reclamación y recurso y de resolución extrajudicial de litigios; así como con alertadores fiables, disponer medidas contra las notificaciones y contranotificaciones abusivas; comprobar las credenciales de terceros proveedores (principio de conocimiento del cliente empresarial); obligaciones de transparencia de la publicidad online para los usuarios; y obligaciones específicas de denuncia de infracciones penales.
- Por último, para los servicios intermediarios de alojamiento de datos que sean plataformas en línea de muy gran tamaño, se añade a todo lo anterior obligaciones sobre gestión de riesgos y responsables del cumplimiento; auditoría externa de riesgos y rendición pública de cuentas; y transparencia de los sistemas de recomendación y posibilidades de elección de los usuarios para el acceso a la información.

desplazará a la normativa sobre intermediarios digitales que se contiene en la propuesta, si bien su contenido seguirá aplicándose –junto al resto de normativa propia de los servicios de la sociedad de la información– en todo aquello no se prevean disposiciones de carácter más específico que les sean aplicables[20].

Asimismo, este régimen de los servicios intermediarios no excluye la aplicación de la normativa general relativa a las actividades que se desarrollan a través de estos servicios intermediarios, como es el caso las normas sobre protección de los consumidores, sobre protección de datos personales, sobre ciberseguridad, sobre condiciones laborales, sobre derechos de autor, entre muchas otras (art. 1.5 Propuesta Ley Servicios Digitales). De hecho, toda esta normativa sustantiva en la que se enmarcan las actividades y contenidos que facilitan los servicios intermediadores resulta esencial en tanto es la que va a determinar que puedan ser considerados ilícitos o no y que los intermediarios tengan que actuar contra los mismos que es, precisamente, lo que pretende reforzar y potenciar esta propuesta de Reglamento de Ley de Servicios Digitales.

IV. NORMAS ESPECÍFICAS SOBRE DETERMINADOS ASPECTOS DE LOS SERVICIOS PRESTADOS EN EL ENTORNO DIGITAL: CONTRATACIÓN DE SERVICIOS DIGITALES, SERVICIOS DE INTERMEDIACIÓN PARA PROFESIONALES Y SERVICIOS DE PLATAFORMAS BÁSICAS

A la normativa horizontal analizada hasta ahora que regula los servicios digitales prestados en línea, se le suma otra normativa que se proyecta sobre aspectos específicos de dichos servicios como son los derechos de los particulares en su contratación (Directiva UE 2019/770), la protección de los usuarios profesionales cuando utilizan grandes plataformas o buscadores como servicios de intermediación (Reglamento UE 2019/1150) o cuando se trata de grandes plataforma (Propuesta de Reglamento de Ley de Mercados Digitales).

Se trata de normas que se focalizan en cuestiones concretas de los servicios digitales, completando así su marco jurídico en tanto se suman a la normativa horizontal analizada hasta ahora aplicándose en esos aspectos, dimensiones o servicios concretos.

[20]En el considerando 9 se indica que la propuesta de Reglamento de Ley de Servicios Digitales «(…) *no afecta a esos otros actos, que han de tener la consideración de lex specialis en relación con el marco de aplicación general establecido en el presente Reglamento. Sin embargo, las disposiciones del presente Reglamento se aplican a problemas que esos otros actos no resuelven, o no por completo, así como a problemas para los que esos otros actos dejan abierta la posibilidad de que los Estados miembros adopten determinadas medidas de ámbito nacional*».

1. La contratación de contenidos y servicios digitales: Directiva (UE) 2019/770

El imparable empuje de la económica digital hizo necesaria la aprobación de una nueva regulación sobre la normativa sobre contratación de los contenidos y servicios digitales contenida en la Directiva (UE) 2019/770 [21]. Se trata de una normativa que se proyecta sobre los derechos de los consumidores cuando contratan bienes y servicios digital en si, y no ya cuando contratan servicios a través de medios digitales, por lo que afecta al marco jurídico específico estos servicios digitales.

En efecto, la Directiva (UE) 2019/770 sobre contratos de suministro de contenidos y servicios digitales tiene como finalidad es armonizar el Derecho contractual a nivel europeo para reforzar la seguridad jurídica de consumidores y empresas para que disfruten de unos derechos comunes en materia de suministro de estos que proporcionen un elevado nivel de protección. Se trata de evitar que los Estados miembros introduzcan diferencias en tres aspectos esenciales como son: la conformidad de los contenidos o servicios digitales con el contrato, las medidas correctoras en caso de falta de conformidad o incumplimiento del suministro, y la modificación de los contenidos o servicios digitales (art. 1).

Por razón de su objeto -los contratos de suministro de servicios digitales[22]– la Directiva (UE) 2019/770 tiene una proyección distinta de la normativa identificada hasta ahora, por lo que no se hace una equiparación de los servicios digitales con los servicios de la sociedad de la información, sino que establece una nueva definición propia y específica de los mismos como aquellos que permiten al consumidor crear, tratar, almacenar o consultar datos en formato digital, o bien que permiten compartir datos en formato digital cargados o creados por el consumidor u otros usuarios de ese servicio, o interactuar de cualquier otra forma con dichos datos (artículo 2.2 Directiva (UE) 2019/770).

Como puede comprobarse, la definición es radicalmente diferente en su planteamiento a la de los servicios de la sociedad de la información ya que prescinde de todos los elementos con los que se definían aquellos y se centra en las actividades sobre los datos digitales. Por lo tanto, la definición de los servicios digitales es más amplia al ser más abstracta, ya que alcanza a supuestos en los que no se desarrolla en línea (como ocurre cuando el servicio –como es un programa de software– se facilita en un soporte material). En todo caso, la definición abarca a la totalidad de los servicios de la sociedad de la

[21] Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales. Esta se complementa con la Directiva (UE) 2019/771, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes.

[22] Sobre el ámbito de aplicación de la Directiva (UE) 2019/770 *vid*. MORAIS CARVALHO (2020: 33-36). También Irati BASOREDO OTZERINJAUREGI (2020: 652-682).

información, como son los servicios en la nube, las redes sociales, los servicios de mensajería instantánea, que siguen sometidos a su régimen específico.

Dado el carácter expansivo de esta normativa sobre contratación de contenido y servicios digitales contenida en la Directiva (UE) 2019/770 se establecen una serie de disposiciones para ajustarla en su aplicación en el resto del ordenamiento jurídico europeo.

Por una parte, se establece una limitación en su ámbito de aplicación a través de una serie de exclusiones, entre las que se encuentran los servicios de telecomunicaciones (excepto los servicios de comunicaciones interpersonales independientes de la numeración –como la mensajería instantánea–, que se analizarán más adelante), los servicios de juego, los servicios financieros, la asistencia sanitaria (artículo 3.5). Asimismo, tampoco se aplica en los supuestos en que el objeto principal del contrato sea la prestación de servicios profesionales (traducción, arquitectura, abogacía, etc.) y tampoco a los servicios públicos, como los de la seguridad social o los registros públicos cuando se utilicen medios digitales (considerando 27).

Por otra, se le dota de un carácter supletorio ya que se dispone expresamente que, en caso de conflicto de cualquiera de sus disposiciones con una disposición de cualquier otro acto de la Unión que regule un sector u objeto específicos, la disposición de ese otro acto de la Unión prevalecerá sobre la Directiva (UE) 2019/770 (art. 3.7).

2. Los servicios de intermediación en línea para usuarios profesionales: Reglamento (UE) 2019/1150

La creciente capacidad de dominio que en este ámbito vienen ejerciendo las grandes plataformas en línea o los principales motores de búsqueda en tanto que elementos esenciales para llegar a los consumidores, han llevado a introducir una nueva regulación a nivel europeo para proteger a los usuarios profesionales en el uso que hacen de estos grandes instrumentos estratégicos.

Con la finalidad de equilibrar la relación entre estos grandes intermediarios estratégicos y los usuarios profesionales se aprobó el Reglamento (UE) 2019/1150 sobre equidad y la transparencia para usuarios profesionales de servicios de intermediación en línea[23] (Reglamento P2B), con el que se introdujo una nueva normativa para determinados servicios de la sociedad de la información que actúan como intermediarios en línea, así como para los motores de búsqueda en línea.

[23] Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.

La finalidad del Reglamento (UE) 2019/1150 es asegurar que se conceden opciones apropiadas de transparencia, de equidad y de reclamación a los usuarios profesionales de servicios de intermediación en línea y a los usuarios de sitios web corporativos en relación con los motores de búsqueda en línea, con la intención última de equilibrar las condiciones de los operadores y garantizar el funcionamiento equilibrado del mercado. Con este objetivo se interviene sobre las condiciones generales que aplican los proveedores de estos servicios, sobre las decisiones de restricción, suspensión y terminación del servicio, sobre el tratamiento diferenciado y otras medidas que pueden afectar a los usuarios profesionales, asegurándoles sistemas de reclamación, mediación y de acción judicial.

Por lo tanto, se trata de una normativa que se aplica exclusivamente a los servicios de intermediación en línea conformes son definidos dentro de los servicios de la sociedad de la información por la Directiva 2000/31/CE a cuya definición se remite el artículo 2.2 Reglamento (UE) 2019/1150. En concreto son aquellos servicios de la sociedad de la información que permiten a los usuarios profesionales ofrecer bienes o servicios a los consumidores, con el objetivo de facilitar el inicio de transacciones directas entre dichos usuarios profesionales y consumidores (con independencia de si se completan en línea, fuera de línea o no lleguen a completarse –por lo que no es necesaria una relación contractual entre los usuarios profesionales y los consumidores–); a lo que se añade, además, que deben prestarse a los usuarios profesionales sobre la base de relaciones contractuales entre el proveedor de los servicios y los usuarios profesionales que ofrecen los bienes o servicios a los consumidores.

Dentro de estos servicios de intermediación interesan exclusivamente aquellos que son contratados por los usuarios profesionales para desarrollar sus actividades económicas y llegar y contratar con los clientes, lo que abarca un creciente catálogo de plataformas en línea como son los mercados de comercio electrónico o los servicios de aplicación de software en línea (tiendas de aplicaciones). En la medida en que la finalidad de estos servicios no sea la de propiciar el inicio de transacciones directas y contratar con los consumidores, quedarán excluidos, como ocurre con los servicios de pagos en línea, las herramientas de publicidad en línea o las plataformas de intercambios publicitarios en línea [art. 1.3 Reglamento (UE) 2019/1150].

Por otra parte, se añaden los motores de búsqueda en línea que se definen como servicios digitales que permiten a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web, o de sitios web en un idioma concreto, mediante una consulta sobre un tema cualquiera en forma de palabra clave, consulta oral, frase u otro tipo de entrada, y que en respuesta muestra resultados en cualquier formato en los que puede encontrarse información relacionada con el contenido solicita [art. 2.5 Reglamento (UE) 2019/1150].

A partir de estas definiciones de los servicios de intermediación en línea y de los motores de búsqueda en línea se determina el ámbito de aplicación del Reglamento (UE) 2019/1150, a los que se aplica un régimen específico para garantizar que los usuarios profesionales dispongan de opciones adecuadas de transparencia, de equidad y de reclamación.

Esta normativa constituye un régimen especial y específico que se aplica preferentemente frente a la normativa horizontal ya sea la propuesta de Reglamento de Ley de Mercados y Servicios Digitales o la Directiva 2000/31/CE, que seguirán aplicándose en todo lo que no disponga de una forma más específica este Reglamento (UE) 2019/1150. Por lo demás, y en tanto que normativa especial, su contenido se entiende sin perjuicio de lo dispuesto en la normativa de carácter general sobre libre competencia, competencia desleal, protección de consumidores, comercio electrónico, protección de datos, secreto comercial que seguirá aplicándose en la medida que no se establezcan previsiones específicas en la misma [art. 1.4 y 5 Reglamento (UE) 2019/1150].

3. Los servicios de plataformas básicas: Propuesta de Ley de Mercados Digitales

De forma paralela a la propuesta de Reglamento de Ley de los Servicios Digitales, y como complemento al Reglamento (UE) 2019/1150 se plantea la propuesta de Ley de Mercados Digitales[24] que se centra en grandes plataformas digitales actúan como puertas de acceso o guardianes de acceso entre los usuarios profesionales y los usuarios finales. En concreto su finalidad es hacer frente a los desequilibrios económicos que generan estas grandes plataformas, las prácticas comerciales desleales de los guardianes de acceso y sus consecuencias negativas, como la reducida disputabilidad de los mercados de plataformas.

Por lo tanto, la propuesta de Reglamento de Ley de Mercados Digitales se centra en determinados servicios digitales, las grandes plataformas en línea de carácter sistémico, que son los que más utilizan los usuarios profesionales y los usuarios finales, para las que establece unas normas armonizadas para garantizar unos mercados disputables y equitativos, en definitiva, más equilibrados y justos. Se trata de los denominados “servicios de plataformas básicas” que son polifuncionales y altamente concentrados por lo que establecen las condiciones comerciales con una autonomía considerable, constituyéndose en puertas de acceso para que los usuarios profesionales lleguen a sus clientes y actúan

[24] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales), presentada el 15.12.2020 COM/2020/842 final. Vid. Apol·lònia MARTÍNEZ NADAL (2021)

como guardianes de acceso utiliza indebidamente su poder dando lugar a que los usuarios profesionales y clientes reciban un tratamiento injusto.

Entre los servicios de plataformas básicas se encuentran las siguientes (art. 2.2 propuesta de Ley de Mercados Digitales): i) servicios de intermediación en línea (incluidos, por ejemplo, mercados, tiendas de aplicaciones y servicios de intermediación en línea en otros sectores como la movilidad, el transporte o la energía), ii) motores de búsqueda en línea, iii) redes sociales iv) servicios de plataformas de intercambio de vídeos, v) servicios de comunicaciones electrónicas interpersonales independientes de la numeración, vi) sistemas operativos, vii) servicios en la nube y viii) servicios de publicidad, incluidas las redes de publicidad, los intercambios publicitarios y cualquier otro servicio de intermediación publicitaria, en los que estos servicios de publicidad estén relacionados con uno o más de los demás servicios de plataformas básicas mencionados anteriormente.

Dentro de los proveedores de servicios de plataformas básicas solamente son relevantes aquellas que constituyen una gran puerta de acceso, constituyéndose así en guardianes de acceso al cumplir los siguientes requisitos (art. 2.1 y 3 propuesta de Ley de Mercados Digitales): i) tienen una posición económica fuerte, un impacto significativo en el mercado interior y actividades en muchos países de la UE; ii) tienen una sólida posición de intermediadora, lo que le permite poner en contacto a una amplia base de usuarios con un gran número de empresas; iii) tienen (o está a punto de tener) una posición arraigada y duradera en el mercado, lo que significa que es estable a lo largo del tiempo. Estos tres criterios se objetivan fijando cuantías concretas de volumen de negocio.

Las obligaciones y prohibiciones que deberán cumplir las grandes plataformas guardianes de acceso se dirigen a garantizar la apertura del mercado. Así se les obliga, en determinados casos, a permitir a terceros a que puedan interactuar con los servicios que prestan; permitir que sus empresas usuarias accedan a los datos que generan al utilizar la plataforma, ofrecer las herramientas y la información necesarias para que los anunciantes y editores de su plataforma lleven a cabo su propia verificación independiente de los anuncios alojados por el guardián de acceso; y permitir que sus empresas usuarias promocionen sus ofertas y celebren contratos con sus clientes fuera de la plataforma del guardián de acceso. Por otra parte, a las plataformas del guardián de acceso se les impide que clasifiquen de forma más favorablemente sus propios servicios y productos que productos o servicios similares ofrecidos por terceros a través de la plataforma; no podrán impedir que los consumidores se pongan en contacto con las empresas fuera de la plataforma del guardián de acceso; y tampoco podrán impedir que los usuarios desinstalen programas o aplicaciones preinstaladas.

De este modo la Propuesta de Ley de Mercados Digitales constituye una normativa especial que establece unas obligaciones adicionales a las ya previstas en el Reglamento

(UE) 2019/1150 específicamente para los servicios de plataformas básicas que tienen la capacidad de afectar a un gran número de usuarios finales y empresas con el consiguiente riesgo de competencia desleal. También se suma a lo dispuesto para los servicios intermediarios en la propuesta de Reglamento de Ley de Servicios Digitales que es una normativa horizontal que trata aspectos generales, mientras que la Ley de Mercados Digitales se ocupa de aspectos específicos como los desequilibrios económicos, las prácticas comerciales desleales de los guardianes de acceso y sus consecuencias. Por lo demás, la Propuesta de Ley de Mercados Digitales constituye una normativa especial que se aplica a los servicios de plataformas básicas, sin perjuicio del resto de la normativa general aplicable como es el caso de la normativa en materia de defensa de la competencia (art. 1.6 propuesta de Ley de Mercados Digitales).

V. LA NORMATIVA SECTORIAL APLICABLE A DETERMINADOS SERVICIOS PRESTADOS EN EL ENTORNO DIGITAL

1. El desarrollo de servicios digitales que desborda los regímenes jurídicos sectoriales: Servicios *over the top* (OTT) y el problema del *playing level field*

La articulación del entorno digital se ha basado en la configuración de distintos sectores –como son las telecomunicaciones (o comunicaciones electrónicas), el audiovisual y los servicios de la sociedad de la información–, que quedan sometidos a unos regímenes jurídicos diferenciados con importantes asimetrías en la intensidad y características de la intervención administrativa desplegada en cada uno de ellos. Se establece así, desde principios de siglo, una ordenación estanca para cada uno de estos sectores que, en un principio, se podían distinguir con claridad, pero cuyas fronteras quedaron rápidamente superadas por los avances tecnológicos que desbordaban las definiciones legales en que se basaba la delimitación de estos sectores.

En efecto, el desarrollo vertiginoso de los servicios digitales en línea prestados a través de Internet durante las dos últimas décadas, impulsados por la mejora en la capacidad y velocidad de conexión y por los avances en la programación informática, ha dado lugar a la aparición de nuevos servicios que dejaron obsoletas las definiciones en que se basaba la delimitación de los distintos sectores en que se articulaba el entorno digital. El alcance de estos cambios se refleja en los denominados servicios *over the top* (OTT), que son servicios prestados sobre Internet directamente a usuarios finales por terceros que utilizan las redes y servicios de comunicaciones electrónicas, sin necesidad de ningún hardware

específico[25]. Pero lo verdaderamente característico de los servicios OTTs es que son servicios que no encajaban en la tradicional definición de los servicios de comunicaciones electrónicas o los audiovisuales, pero prestaban las mismas funcionalidades, compitiendo en el mercado con éstos desde un régimen jurídico distinto y mucho menos exigente como es el propio de los servicios de la sociedad de la información.

Así, frente a los servicios de comunicaciones electrónicas, van surgiendo servicios OTT de mensajería instantánea que permite el envío de texto, imágenes y videos (WhatsApp, Telegram, Line, etc.) que sustituyen servicio de telecomunicaciones similares (como los mensajes de SMS o MMS). También van extendiéndose servicios de audio o videollamada (como el propio WhatsApp, Skype, Zoom, etc.) que, cada vez más, sustituyen a los tradicionales servicios de telefonía vocal. En la medida en que todos estos servicios dependen del servicio de acceso a Internet, los demás servicios de telecomunicaciones van siendo abandonados progresivamente a favor del servicio de banda ancha fija o móvil, que es lo único y fundamental que necesitan los usuarios en esa convergencia al todo IP.

Por otra parte, respecto a los servicios de comunicación audiovisual, estos servicios OTT van concentrando cada vez una mayor audiencia en las nuevas formas de consumo de contenidos audiovisuales que superan a los tradicionales canales difusión a través de los servicios de radio y televisión. Se trata de plataformas de video bajo demanda en *streaming* como Netflix, HBO, Amazon Prime que no son meros difusores sino creadores de contenidos y, por tanto, actores plenos del sector audiovisual, así como plataformas de intercambios de videos o de retransmisión en directo o en diferido como Youtube, Vimeo o Twitch.

Por último, aunque no suele identificarse como servicios OTT, también han surgido innumerables servicios prestados a través de Internet (servicios de la sociedad de la información) que están alterando todos los sectores económicos ya que surgen como instrumentos que modifican el esquema de los mercados de bienes y de servicios. Estos aparecen ofreciendo funcionalidades complementarias a los actores de esos mercados (como los comparadores de productos o las plataformas de prestadores de servicios) o como actores alternativos (distribución de productos -como supermercados- o de prestación de servicios -apps de seguros-). Esta incidencia tiene un mayor alcance en aquellos sectores que se encuentran sometidos a una mayor intervención pública, pues los nuevos servicios ofrecidos en línea son sustitutivos de los ya existentes, pero no están sometidos a las limitaciones y exigencias propias de la regulación de ese sector –por lo

[25] Al respecto se puede consultar el "Report on OTT Services"del BEREC [BoR (16) 35] de 29 de enero de y, asimismo, "Caracterización del uso de algunos servicios over the top en España (servicios de comunicaciones y servicios audiovisuales)", Documento de Trabajo nº 4 de la CNMC, diciembre 2014. Por extenso *vid.* VIDA FERNÁNDEZ (2021)

que operan en la misma lógica "*over the top*" que los servicios OTT–, como se ha puesto de manifiesto en el caso del sector del transporte de pasajeros (con iniciativas como Uber, Cabify) o en el de los alojamientos (como AirBnB, Booking).

Como se puede comprobar, el desafío de los nuevos servicios digitales es común para la articulación jurídica de los sectores del entorno digital como para el resto de sectores económicos, en tanto desbordan las definiciones legales de modo que no les resulta aplicable el régimen jurídico específico previsto para cada sector, a pesar de que actúan como actores relevantes de los mismos. Este desequilibrio ha sido denunciado por los operadores tradicionales de los correspondientes sectores (comunicaciones electrónicas, audiovisual, transportes, alojamiento, etc.) que ha venido reclamando el denominado *level playing field* para competir en pie de igualdad con estos servicios digitales que se benefician de las insuficiencias en la articulación del régimen jurídico, eludiendo las obligaciones, exigencias y cargas previstas en el mismo.

A pesar del desafío que suponía la aparición de estos nuevos servicios OTT para la articulación jurídica de los distintos sectores, las definiciones legales sobre las que establecía la delimitación de cada uno de estos sectores han permanecido sorprendentemente inalteradas durante casi dos décadas, desde los inicios de siglo[26]. Ante la renuncia por parte del legislador europeo de abordar la cuestión, fue la jurisprudencia del Tribunal de Justicia de la Unión Europea la que ha venido a concretar y aclarar las dudas en una serie de sentencias que han sido tenidas en cuenta posteriormente por el legislador europeo a la hora de definir los distintos tipos de servicios del ámbito digital.

Sin embargo, se trata de un problema complejo que carece de una solución única y definitiva, y que se ha abordado eludiendo las alternativas binarias que llevan a aplicar uno u otro régimen jurídico. Por el contrario, en sectores como las comunicaciones electrónicas y el audiovisual se ha optado por ampliar el ámbito de aplicación de los mismos para abarcar los servicios que operaban fuera de los mismos, aunque quedan sometidos a unas obligaciones específicas y más flexibles que las propias de los operadores tradicionales del sector para permitir su desarrollo a la vez que se garantizan los objetivos de interés general.

[26] En efecto, si bien la Directiva Marco y el resto del Paquete Telecom de 2002 fue modificada por la Directiva 2009/140, sin embargo, no se modificaron las definiciones de los servicios de comunicación electrónica. Otro tanto sucedió con los servicios de comunicación audiovisual una vez que fueron introducidos en la Directiva 2007/65/CE y a la que sustituyó la Directiva 2010/13/UE sobre servicios de comunicación audiovisual. Tampoco se modificó la definición de los servicios de la sociedad de la información asentada en la Directiva 98/34/CE que fue sustituida por la Directiva 2015/1535.

2. Servicios digitales que son servicios de comunicaciones electrónicas: Directiva (UE) 2018/1808, de Código Europeo de Comunicaciones Electrónicas

El sector de las telecomunicaciones, en tanto que se encuentra sometido a una intensa regulación, ha sido el más afectado por el impacto de los servicios digitales en línea que prestan funcionalidades sustitutivas a las de los operadores tradicionales, acuñándose el concepto de operadores *over the top* (OTT). Estos OTTs han creado un importante desequilibrio al concurrir en un mismo mercado operadores que se encuentran sometido a regímenes jurídicos asimétricos, por lo que se ha procurado equilibrar la situación entre estos operadores, extendiendo la condición de operadores de telecomunicaciones a estos servicios OTT, a los que se aplica un régimen menos exigente.

Para comprender mejor este problema y las soluciones que se están arbitrando, se debe tener en cuenta la evolución que se ha producido en el ámbito de aplicación de la normativa de telecomunicaciones y cómo ha sido modulado por el empuje de los servicios digitales prestados por Internet que operan como OTTs[27].

Así debe tenerse en cuenta que, originariamente, cada servicio de telecomunicaciones se prestaba a través de una red concreta hasta que la irrupción de la digitalización y la conmutación por paquetes, que dio paso a la liberalización, permitió que los servicios de telecomunicaciones se pudiesen ofrecer a través de distintas redes. Se proyecta así una regulación convergente en cuanto a los medios de transmisión –ya que habían estado sometidos a regímenes dispares (telefonía, cable, satélite, etc.)–, sometiéndose a un mismo régimen jurídico a las actividades de transmisión de señales independientemente de los contenidos transmitido.

Este cambio se acompañó, a nivel europeo, de una nueva denominación en las directivas del Paquete Telecom de 2002, ya que se abandona el término telecomunicaciones y se pasa a hacer referencia a las comunicaciones electrónica, que se componen de redes, servicios y recursos asociados. En concreto, los servicios de comunicaciones electrónicas se definieron en aquel momento como aquellos servicios prestados, por lo general a cambio de una remuneración que consisten, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas (artículo 2 a) Directiva 2002/21/CE, Directiva Marco[28]).

[27] Un análisis en profundidad sobre esta cuestión puede encontrarse en VIDA FERNÁNDEZ (2021).

[28] Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco).

La convergencia sobre las comunicaciones electrónicas[29] afectó sólo al régimen de las transmisiones y no de los contenidos transmitidos que siguieron sometidos a regímenes diferenciados como servicios audiovisuales o servicios de sociedad de la información. Se mantiene así un sistema de regímenes jurídicos estancos, basados en unas definiciones que se han mantenido inalteradas durante casi dos décadas, por lo que ha sido el TJUE el que vino a aclarar, por una parte, que el servicio de correo electrónico no es un servicio de comunicaciones electrónicas sino un servicio sociedad de la información, y que determinado servicio en línea de llamadas directas a teléfonos convencionales es un servicio de comunicaciones electrónicas[30].

Esta jurisprudencia ha sido tenida en cuenta en la configuración del Código Europeo de las Comunicaciones Electrónicas aprobado por la Directiva (UE) 2018/1972 [31], que amplia la definición de los servicios de comunicaciones electrónicas para incluir servicios de la sociedad de la información que habían quedado fuera de dicha consideración. Sin embargo, no incorporan en pie de igualdad ya que se establecen tres categorías con regímenes específicos y asimétricos: servicios de acceso a internet, los servicios de comunicaciones interpersonales, y los servicios que consisten total o principalmente en el transporte de señales.

Dentro de los servicios de comunicaciones interpersonales[32] se distinguen entre aquellos basados en numeración, entre los que se encuentran los servicios de comunicación vocal, y los independientes de la numeración, que son la verdadera novedad, ya que supone la inclusión de un gran número de servicios de la sociedad de la información. Lo relevante de esta nueva categoría es que quedan sometidas a un tratamiento jurídico diferenciado mucho menos exigente, ya que estos últimos sólo deben estar sujetos a obligaciones cuando el interés público exija la aplicación de obligaciones reglamentarias.

---

[29] Vid. Belén ANDRÉS SEGOVIA (2020).

[30] En la STJUE de 13 de septiembre de 2019, C-193/18, se pronuncia sobre con respecto al servicio de correo electrónico de Google confirmando que no se trata de un servicio de comunicaciones electrónicas, y en la STJUE de 5 de junio de 2019, C-142/18, se refiere a un servicio de llamadas de Skype Out directamente a teléfonos fijos o móviles, es considerado parte de los servicios de comunicaciones electrónicas.

[31] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

[32] Se definen como los prestados por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio (artículo 2.5 CECE).

En todo caso, estos nuevos servicios de comunicaciones interpersonales no basadas en numeración no abandonan el régimen de los servicios de la sociedad de la información y el resto de la normativa de los servicios de intermediación y plataformas básicas, que se les seguirá aplicando en la medida que no quede desplazado por la normativa de las comunicaciones electrónicas que actuará como *lex specialis*.

3. Servicios de comunicación audiovisual: Directiva (UE) 2018/1808 de servicios de comunicación audiovisual

Por lo que respecta a los servicios audiovisuales, estos han contado con una normativa propia que, a nivel europeo, se remonta a la Directiva 89/552/CEE (de televisión sin fronteras)[33], en la que se parte de la identificación de la actividad de radiodifusión por razón de la tecnología de transmisión analógica que era en un solo sentido de forma simultánea a una multiplicidad de usuarios (punto-multipunto), por lo que denominaban como "medios de difusión" y los convertía en medios de comunicación de masas, lo que justificaba que estuvieran sometidos a un régimen jurídico específico y distinto del régimen de las telecomunicaciones, ya que estas permitían una comunicación interactiva punto a punto como ocurría con la telefonía vocal o el telégrafo.

La convergencia derivada del avance tecnológico llevó a que los contenidos audiovisuales pudiesen transmitirse a través de distintos tipos redes y que esas mismas redes pudiesen transmitir cualquier tipo de contenidos, haciendo que fuese cada vez más difícil la distinción de los servicios audiovisuales –como la emisión en directo en tiempo real por Internet (*live streaming*), la difusión web (*webcasting*) y el vídeo casi bajo demanda– de los servicios de comunicaciones electrónicas y de los servicios de la sociedad de la información. Esto es lo que condujo a la integración de las redes de radiodifusión sonora y televisiva, en cuanto sistemas de transmisión, en las redes de comunicaciones electrónicas conforme a la regulación convergente, aunque se mantuvo la regulación de los contenidos transmitidos en la normativa audiovisual bajo la nueva definición de los "servicios de comunicación audiovisual" que introdujo la Directiva 2007/65/CE de modificación de la Directiva de televisión sin fronteras.

Los servicios de comunicación audiovisual pasan a definirse como aquellos cuya responsabilidad editorial corresponde a un prestador del servicio de comunicación y cuya principal finalidad es proporcionar programas, con objeto de informar, entretener o educar

[33] En la Directiva 89/552/CEE del Consejo, de 3 de octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados Miembros relativas al ejercicio de actividades de radiodifusión televisiva, se definía la radiodifusión televisiva como la emisión primaria, con o sin hilo, por tierra o por satélite, codificada o no, de programas televisados destinados al público (art. 1 a).

al público en general, a través de redes de comunicaciones electrónicas, independientemente de si es o no bajo demanda, e incluyendo comunicaciones comerciales[34]. Esta definición se centra en la consideración de que estos servicios de comunicación audiovisual son medios de comunicación de masas, es decir, que están destinados a una parte significativa del público en general y que puedan tener un claro impacto sobre él en el ejercicio de su función de informar, entretener y educar al público general, así como de emitir comunicaciones audiovisuales comerciales[35]

Por lo tanto, y tal y como ha confirmado la jurisprudencia del TJUE[36], quedan excluidos de los servicios de comunicación audiovisual aquellos que impliquen actividades que no sean fundamentalmente económicas, ni entren en competencia con la radiodifusión televisiva, ni los servicios cuyo principal objeto no sea proporcionar programas, es decir, aquellos cuyo contenido audiovisual sea meramente incidental y no constituya la finalidad principal, situación en la que encajan multitud de servicios de sociedad de la información. Asimismo, quedan excluidas las redes y servicios de comunicaciones electrónicas utilizados para el transporte y difusión de la señal de los servicios de comunicación audiovisual, sus recursos asociados y los equipos técnicos necesarios para la recepción de la comunicación audiovisual, en tanto su régimen es el propio de las telecomunicaciones.

La Directiva (UE) 2018/1808[37] de servicios de comunicación audiovisual ha venido ha modificar el alcance de esta normativa por razón de la convergencia de la televisión y los servicios de internet gracias a los avances técnicos que ofrecen nuevos servicios que modifican los hábitos de los ciudadanos, que van abandonando los contenidos televisivos tradicionales a través de la pantalla de televisión por nuevos tipos de contenidos, como los vídeos cortos o el contenido generado por los usuarios, al margen de los servicios de vídeo a petición.

---

[34] Artículo 1 a) de la Directiva 89/552/CEE, modificada por la Directiva 2007/65/CE.

[35] Directiva 2007/65/CE, Considerandos 16 y 18. Vid sobre la evolución G. AGUADO-GUADALUPE; I. BERNAOLA, I. (2019: 13-34).

[36] La STJUE de 13 de diciembre de 2018, C-298/17, deja fuera de la consideración de servicios de comunicación electrónica la oferta de contenidos audiovisuales a través de Internet, similar a la que llevan a cabo multitud de plataforma de video bajo demanda, ya que una cosa es la transmisión y otra el contenido de los servicios prestados a través de las redes y servicios de comunicaciones electrónicas. Por otra parte, la STJUE de 7 de noviembre de 2013, C-518/11 y en la STJUE de 30 de abril de 2014, C-475/12 calificó como operador de comunicaciones electrónicas a un operador de cable que facturaba tanto por los costes de transmisión como por los derechos de autor y un servicio de conexión vía satélite que ofrecía esencialmente contenidos televisivos de acceso condicional.

[37] Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado.

Así se ajusta la definición de los servicios de comunicación audiovisual, ya que se parte de la tradicional identificación de estos servicios como aquellos cuya finalidad consiste en ofrecer programas al público en general, bajo la responsabilidad editorial de un prestador de servicios de comunicación, con objeto de informar, entretener o educar, a través de redes de comunicaciones electrónicas, pero se especifica que debe ser su finalidad principal propia o de una de sus partes disociables[38].

No obstante, lo verdaderamente novedoso es la inclusión en la normativa audiovisual de los servicios de intercambio de vídeos a través de plataforma o plataformas de intercambio de vídeos que son definidos como aquellos cuya finalidad principal propia o de una de sus partes disociables o cuya funcionalidad esencial consiste en ofrecer al público en general programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretener o educar, a través de redes de comunicaciones electrónicas, y cuya organización determina el prestador de la plataforma de intercambio de vídeos, entre otros medios con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación[39].

Estos servicios y plataformas de intercambios de videos quedan sometidos a un régimen jurídico específico que se construye sobre el régimen propio de los servicios de comunicación audiovisual, aunque limitando y modulando el alcance de muchas de las obligaciones, requisitos y exigencias dispuestos para estos últimos, sometiéndolos así un marco jurídico mucho más flexible.

En todo caso, la normativa sobre servicios de la sociedad de la información, servicios intermediarios y plataformas básicas seguirá aplicándose a estos servicios audiovisuales ya que la Directiva (UE) 2018/1808 funge también como *lex specialis* en lo que respecta a contenidos audiovisuales y comunicación comercial audiovisual, y no desplazará a la normativa común horizontal en tanto no contengan disposiciones de carácter más específico que les sean aplicables.

---

[38] Conforme a la nueva redacción del artículo 1.1 a) de la Directiva 2010/13/UE. Se cumple el requisito del objetivo principal si el servicio tiene una forma y contenido audiovisuales disociables de la actividad principal del prestador de servicios, como las partes autónomas de los periódicos en línea que ofrecen programas audiovisuales o vídeos generados por usuarios, cuando dichas partes puedan considerarse disociables de su actividad principal. Por el contrario, se trata de un mero complemento indisociable de la actividad principal cuando exista una conexión importante entre la oferta audiovisual y la actividad principal, como facilitar noticias por escrito [considerando 3 de la Directiva (UE) 2018/1808]

[39] Conforme a la nueva redacción del artículo 1.1 a) bis de la Directiva 2010/13/UE. Lo que se justifica en tanto se ponen a disposición contenidos audiovisuales y se han convertido en un importante medio para compartir información, entretener y educar, y compiten por la misma audiencia e ingresos que los servicios de comunicación audiovisual, además de tener un impacto considerable, ya que ofrecen a los usuarios la posibilidad de conformar las opiniones de otros usuarios e influir en ellas.

4. Servicios digitales de intermediación que son parte integrante de otros servicios sometidos a normas sectoriales (servicios de alojamiento, transporte y otros)

Los servicios digitales en línea han impactado sobre la totalidad de las actividades económicas, si bien han afectado más a aquellos sectores sometidos a una intervención más intensa ya que se los prestadores de estos servicios se han incorporado a estos sectores eludiendo el cumplimiento de las exigencias impuestas a sus operadores, lo que les ha permitido como verdaderos operadores OTT[40].

Uno de los sectores que más se ha visto afectado por estos servicios digitales ha sido el transporte, tanto de personas como de mercancías, sobre el que precisamente se ha pronunciado el TJUE para determinar si estos servicios digitales que actúan como intermediarios en la prestación de estos servicios deben considerarse o no servicios de transporte[41].

En este sentido, el TJUE ha interpretado que estos servicios dejan de ser simples servicios de sociedad de la información, y pasan a ser considerado otro tipo de servicio (de transporte, alojamiento, etc.) sometiéndose a su régimen jurídico, cuando en función de las características del servicio de intermediación que cumplen y de cómo se insertan y afecta a la estructura de prestación del servicio final para el que realizan la intermediación, ese servicio de intermediación forme parte integrante de un servicio global cuyo elemento principal sea un servicio al que corresponda otra calificación jurídica (servicio de transporte, de alojamiento, etc.)

Este es el criterio que se fijó en la conocida STJUE de 20 de diciembre de 2017, C-434/15, *Asociación Profesional Élite Taxi contra Uber Systems Spain, SL*. consideró que un servicio de intermediación para la prestación de servicio de transporte de vehículos de turismo con conductor (VTC) como Uber no era un simple servicio de la sociedad de la información, en tanto el prestador crea una oferta de servicios de transporte urbano, que hace accesible concretamente mediante herramientas informáticas, y organiza el funcionamiento general de la misma en favor de las personas que deseen recurrir a esta oferta, por lo que el servicio de intermediación prestado debe considerarse parte integrante de un servicio global cuyo elemento principal es un servicio de transporte y, por lo tanto, pasa a ser considerado un servicio de transporte y a someterse a la normativa de los mismos.

---

[40] Sobre esta cuestión vid. Ana María DE LA ENCARNACIÓN VALCÁRCEL; Andrés BOIX PALOP (2018), y, asimismo, Lucía VÁZQUEZ-PASTOR JIMÉNEZ (2021)

[41] Sobre las plataformas de transporte colaborativo y los VTC *vid.* Gabriel DOMÉNECH PASCUAL (2021). Desde una perspectiva general vid. Ana María TOBÍO RIVAS (2021).

Este mismo criterio ha sido aplicado en otros ámbitos, como ha sido el caso de los servicios de intermediación de alojamiento en la STJUE de 19 de diciembre de 2019, C-390/18, *Airbnb Ireland UC*,[42]. en la que se llega a la conclusión de que la actividad de intermediación de Airbnb, es un simple servicio de la sociedad de la información, en la medida en que el arrendador y el arrendatario son puestos en contacto a través de una plataforma electrónica en la que no se requiere la presencia simultánea del prestador del servicio de intermediación, por un lado, y del arrendador o el arrendatario, por otro, a lo que se añade que el servicio de Airbnb no es indispensable para la realización de prestaciones de alojamiento al existir otros cauces alternativos, por lo que sometida al principio de libre prestación y no se le puede exigir los requisitos propios de los agentes inmobiliarios.

Este planteamiento puede proyectarse en cualquier otro sector en el que exista una normativa completa y acabada que contenga una intervención intensa disponiendo requisitos y obligaciones relevantes, y en el que los servicios de la sociedad de la información operen como servicios intermediarios incidiendo de forma determinante en la actividad desarrollada dentro del mismo, como ocurre en caso de los servicios financiero, de seguros, del juego, farmacéuticos, de seguridad, entre otros. En la medida que los servicios intermediarios puedan considerarse parte integrante de un servicio global cuyo elemento principal es el servicio regulado, pasará a ser considerado como el servicio de que se trate y sometido a su regulación.

Se puede apreciar así la existencia de una frontera muy difusa entre los servicios digitales y los servicios regulados y que obliga a realizar una operación de distinción muy compleja y casuística ya que depende del sector de que se trate y de la definición que se haga del servicio regulado en cuestión, así como de la configuración del servicio intermediario que opera en el mismo.

VI. CONCLUSIONES

La imparable expansión y desarrollo de los servicios digitales prestados a través de Internet está dando lugar a un incremento de la normativa que los regula, con la que se trata de hacer frente a los novedosos y complejos problemas que van surgiendo. Sin embargo, toda esta normativa que se esta aprobando a nivel europeo tiene un carácter específico y aborda cuestiones concretas, aunque se apliquen de forma generalizada.

El resultado es que los servicios digitales se encuentran sometidos a una amalgama de normas que no se encuentran ajustadas, sino que se aplican “sin perjuicio de las

[42] Un comentario a la misma se encuentra en José Ignacio CUBERO MARCOS (2020) y Ricardo PAZOS CASTRO (2020)

demás" –tal y como suelen indicar en su articulado– lo que puede interpretarse en el sentido más pleno de la expresión, ya que se adoptan unas a espaldas de las otras.

Este desajuste entre las normas que componen el marco jurídico de los servicios digitales se manifiesta en la propia terminología ya que, se parte de los servicios de sociedad de la información y, a partir de ahí surgen un sinfín de conceptos como servicios intermediarios, servicios de plataformas básicas, y esto al margen de que ni siquiera se definen legalmente los servicios digitales.

La falta de una definición común y sistemática de los servicios implicados da lugar a una dificultad en la determinación del ámbito de aplicación de las normas que se refiere a estos servicios. Asimismo, estas normas se disponen conforme a dos modalidades que no siempre están claramente definidas, ya que, unas veces las normas se disponen por capas por lo que se van sumando desde las normas más genéricas a las más específicas sobre servicios o aspectos concretos de éstos. Mientras que en otros supuestos se introducen como normas especiales que desplazan al resto de la normativa constituyéndose en la única normativa aplicable para ciertos servicios.

A todo esto se añade que los contornos de estas normas y su respectivo encaje no están bien definidos, a lo que se suma la difusa distinción entre algunos de los servicios implicados lo que provoca que no se sepa a qué régimen jurídico queda sometido.

El resultado es que los operadores jurídicos encuentran verdaderas dificultades para concretar el régimen jurídico aplicable para un servicio concreto, por lo que resulta imprescindible identificar toda la normativa relevante para los servicios digitales y sistematizarla para conocer la relación que existen entre las distintas normas y cómo interactúan, tal y como se lleva a cabo a lo largo del presente trabajo.

Por lo tanto, resulta urgente que se lleve a cabo una labor de codificación de toda la normativa regladora de los servicios digitales, pero no para dar lugar a una norma única y homogénea sino para que la normativa que compone su régimen jurídico tenga mayor coherencia y sistemática que aporte una mayor eficacia y seguridad jurídica.

VII. BIBLIOGRAFÍA

AGUADO-GUADALUPE, G. y BERNAOLA, I. (2019). «El nuevo marco regulador europeo de los servicios audiovisuales bajo petición y de intercambio de vídeo. Su repercusión en el mercado español de plataformas», *Index.Comunicación*, 9(3), 13-34.

ÁLVAREZ MORENO, María Teresa (2020): *La contratación electrónica mediante plataformas en línea: Modelo negocial (B2C), régimen jurídico y protección de los contratantes (proveedores y consumidores)*, Reus.

ANDRÉS SEGOVIA, Belén: *La convergencia de las telecomunicaciones, los medios de comunicación y las tecnologías de la Información*, Aranzadi, 2020.

BASOREDO OTZERINJAUREGI, Irati (2021): «Derecho aplicable al contrato de suministro de contenidos y servicios digitales», en Pilar JIMÉNEZ; Ángel ESPINIELLA MENÉNDEZ (dirs.), *Nuevos escenarios del derecho internacional privado de la contratación*, págs. 652-682.

CASTELLÓ PASTOR, José Juan (2021): «Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales», en CASTELLÓ PASTOR, José Juan (dir.), *Desafíos jurídicos ante la integración digital aspectos europeos e internacionales*, Aranzadi-Thomson Reuters, págs. 37-76.

CORDERO ÁLVAREZ, Clara Isabel (2021), «Plataformas digitales: nuevos retos conceptuales para el Derecho internacional privado europeo de consumo», en CASTELLÓ PASTOR, José Juan (dir.), *Desafíos jurídicos ante la integración digital aspectos europeos e internacionales*, Aranzadi-Thomson Reuters, págs. 77-108.

CUBERO MARCOS, José Ignacio (2020): «¿Plataformas de intermediación, arrendadores de viviendas o agentes inmobiliarios?, Comentario a la sentencia del tribunal de justicia de la Union Europea de 19 de diciembre de 2019 (gran sala)», *Revista española de derecho administrativo*, Nº 209, págs. 255-276.

CUENA CASAS, Matilde (2020), «La contratación a través de plataformas intermediarias en línea», *Cuadernos de derecho transnacional*, Vol. 12, Nº. 2.

DE LA ENCARNACIÓN VALCÁRCEL, Ana María (dir.); BOIX PALOP Andrés (coord.) (2018), *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español*, Aranzadi Thomson Reuters.

DOMÉNECH PASCUAL, Gabriel (2019), «Penalty y expulsión. La economía de las plataformas digitales en el sector de los taxis y los VTC», en Gemma RUBIO GIMENO (dir.), Antonio ORTI VALLEJO (dir.), *Propuestas de regulación de las plataformas de economía colaborativa: perspectiva general y sectoriales*, págs. 293-310, Nº. 15

ECHEBARRÍA SÁENZ, Marina (2021). «Restricciones de acceso al mercado y plataformas digitales: el caso Amazon como ejemplo», *Revista de Estudios Europeos*, No 78, julio-diciembre, 2021,154-182.

FERNÁNDEZ, Lionel. «El Código Europeo de las Comunicaciones Electrónicas: Una auténtica reforma de la regulación de las telecomunicaciones», *Revista General de Derecho de los Sectores Regulados*, 2-9.

FERNÁNDEZ CHACÓN, Ignacio (2020), «El ámbito material de la aplicación de la nueva Directiva relativa a los contratos de suministro de contenidos y servicios digitales aspectos clave», en Luis Antonio FERNÁNDEZ VILLAZÓN (coord.), *Derecho y nuevas tecnologías*, 2020, págs. 559-586.

GARCÍA GOLDAR, Mónica (2020) «Plataformas para el suministro de contenidos y servicios digitales: reflexiones de la Directiva (UE) 770/2019», en Apol·lònia Martínez Nadal (dir.), *Plataformas digitales: aspectos jurídicos*, Aranzadi, págs. 83-113.

MALARET GARCÍA, Elisenda. (2015). «Los servicios excluidos del ámbito de aplicación de la legislación de telecomunicaciones: Los servicios de la Sociedad de la Información y los Servicios de Comunicación Audiovisual», en T. QUADRA-SALCEDO (Dir.), J. VIDA (coordinador), Derecho de las telecomunicaciones, Aranzadi, Cizur Menor,, págs. 104-137.

MARTÍNEZ CALVO, Javier (2021): «Los datos personales como posible contraprestación en los contratos de suministro de contenidos y servicios digitales», *Indret: Revista para el Análisis del Derecho*, Nº. 4.

MARTÍNEZ NADAL, Apol·lònia (2021), «La Propuesta de Reglamento de Mercados Digitales ("Digital Markets Act"): una aproximación jurídica», en Apol·lònia Martínez Nadal (dir.), *Plataformas digitales: aspectos jurídicos*, Aranzadi.

MORAIS CARVALHO, Paulo (2020) «Introducción a las nuevas Directivas sobre contratos de compraventa de bienes y contenidos o servicios digitales», en Esther ARROYO AMAYUELAS; Sergio CÁMARA LAPUENTE (dirs), *El Derecho Privado en el nuevo paradigma digital*, Marcial Pons, págs. 31-47

PAZOS CASTRO, Ricardo (2020): «Uber, Airbnb y la llamada «influencia decisiva» de las plataformas digitales», *IDP: revista de Internet, derecho y política*, Nº. 31.

RODRÍGUEZ DE LAS HERAS Ballell, Teresa (2021), «Las plataformas: nuevos actores (y reguladores) de la actividad económica», *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, Nº. Extra 3, 2021 (Ejemplar dedicado a: Derecho y política ante la pandemia: Reacciones y transformaciones. Tomo II. Reacciones y transformaciones en el Derecho Privado), págs. 403-417.

TOBÍO RIVAS, Ana María (2021) *Las plataformas electrónicas de transporte terrestre de personas y su configuración jurídica*, Reus.

VÁZQUEZ-PASTOR JIMÉNEZ, Lucía (2021), «La disrupción de la economía colaborativa en el sector del alojamiento turístico: el caso AIRBNB. Comentario a la STJUE de 19 de diciembre de 2019 (TJCE 2019, 302)», Revista Aranzadi de derecho patrimonial, Nº 53.

VIDA FERNÁNDEZ, José (2021), «La articulación jurídica del entorno digital: Insuficiencias y soluciones en la delimitación de los sectores de referencia ante el desafío de los servicios over the top (OTT)», *Revista de Derecho Administrativo* – CDA, núm. 20.

ZURIMENDI, Aitor; FERNÁNDEZ GARCÍA DE LA YEDRA, Ainhoa (2020), «Naturaleza jurídica de las plataformas digitales», *Revista General de Derecho de los Sectores Regulados*: Nº. 6.

LOS MERCADOS DE PLATAFORMAS DIGITALES: ENTRE EL DERECHO DE LA COMPETENCIA Y LA REGULACIÓN

Por

CARMEN RODILLA MARTÍ
Prof. Cont. Dr. Departamento de Derecho Mercantil "Manuel Broseta Pont"
Universidad de Valencia

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

RESUMEN: En este trabajo se aporta una visión amplia del papel de los distintos instrumentos de Derecho de la competencia (regulatorio) y la regulación para hacer frente, tanto a los fallos estructurales y de mercado, como a las conductas anticompetitivas de determinados operadores conocidos como guardianes del mercado. Se concluye que una aproximación tradicional y exclusiva del Derecho de la competencia es insuficiente para resolver los problemas. Se recomienda alterar el paradigma de bienestar del consumidor para sustituirlo por el mercado en competencia, más próximo a las tesis ordoliberales europeas, igual que se subraya la relevancia de prestar atención a la ola de concentraciones existente en estos mercados digitales. Finalmente, se recomienda adoptar un fuerte impulso regulatorio donde prime la "precautionary approach"

PALABRAS CLAVE: Derecho de la competencia, mercados digitales, plataformas, dominancia, regulación, concentraciones.

SUMARIO: I. INTRODUCCIÓN Y CARACTERÍSTICAS DE LOS OPERADORES. II. TRATAMIENTO JURÍDICO DE LA CUESTIÓN. 2.1. Antitrust. 2.1.1. La teoría del daño. 2.1.2. La efectividad de la aplicación del Derecho de la competencia: estándar de prueba e intervención ex post. 2.1.3. Definición del mercado relevante. 2.2. Regulación. 2.2.1. El freno a la innovación. 2.2.2. Fortalezas de la regulación. 2.3. Derecho de la competencia regulatorio. III.CONCLUSIONES. IV. BIBLIOGRAFÍA.

DIGITAL PLATFORMS' MARKETS: BETWEEN COMPETITION LAW AND REGULATION

ABSTRACT: This paper aims at presenting a broad vision of the (regulatory) antitrust and regulation tools that the legislator may use in order to address not only structural and market failures, but also anticompetitive conducts by certain market players known as gatekeepers. We conclude that a traditional competition law approach is insufficient for solving the problems arising in these new markets. We recommend the adoption of a new paradigm for the enforcement of competition law. Consumer welfare should be replaced by the proper functioning of a plural market, closer to the ordoliberal European tradition. Additionally, we highlight the relevance of the scrutiny of mergers in the digital sector. Finally, we suggest the adoption of a strong regulatory impulse stressing the "precautionary approach"

KEYWORDS: Antitrust, digital markets, platforms, dominance, regulation, mergers.

I. INTRODUCCIÓN Y CARACTERÍSTICAS DE LOS OPERADORES

La existencia y funcionamiento de los mercados digitales ha generado enormes beneficios para la sociedad, en general, y los consumidores y empresas, en particular, que han de ser, sin duda, potenciados. Entre estos figurarían el incremento de la innovación y la eficiencia, pero también la expansión de la base de consumidores a los que se puede acceder, que ha venido facilitado por la visibilidad en plataformas digitales.

El aumento de la innovación ha de predicarse, por supuesto, a la creación de nuevos mercados (como ha sucedido con plataformas de captación de atención de los consumidores, como pueda ser Facebook), pero, también se ha de predicar el incremento o mejora de la innovación respecto de nuevas formas de operar en el mercado (el hecho de que exista una plataforma en la que poner a la venta productos o servicios no es algo novedoso, pero sí lo es hacerlo masiva e internacionalmente a través de internet).

Respecto del segundo efecto, y casi más importante respecto de los beneficios que supone para los consumidores, es la introducción de un mayor nivel de eficiencia en el funcionamiento de los mercados, los creados *ex novo*, pero también los ya existentes. Esta forma de operar en los mercados a través de grandes plataformas ha contribuido a reducir inmensamente los costes de transacción, aunque no tanto los de información (al menos para aquéllos que se relacionan con la plataforma), en torno a los cuales sigue existiendo un relevante desequilibrio en los datos que controla el operador dominante del mercado digital y aquéllos que tienen los que se relacionan con ella a ambos lados: tanto oferentes de bienes y servicios como demandantes.

Siendo lo anterior cierto, y debido al poder de mercado adquirido como gestores de estos mercados, no se puede negar que los grandes operadores de estos mercados también han contribuido a producir una serie de desajustes y son responsables de ciertas conductas, como mínimo, sospechosas que están siendo investigadas por la Administración y, en algunos supuestos, también han sido sancionadas por las autoridades de competencia.

Estas últimas, tanto las europeas como sus homónimas norteamericanas, han iniciado una campaña de análisis, revisión y escrutinio del sector digital, de la que se han derivado numerosas decisiones sancionadoras que afectan a los gigantes tecnológicos, en general apelados como *big tech*, entre los que se encuentran empresas de la talla de Amazon, Apple, Microsoft, Facebook y Google. Se trata, esencialmente, de una serie de conductas de abuso de posición de dominio y de monopolización (e, incluso, en algunos

casos, de abuso de dependencia económica[1]), cuyo resultado es el de perjudicar directa e indirectamente a los consumidores, esencialmente, aunque también, a los trabajadores, clientes y proveedores e, incluso, la propia estructura del mercado.

En realidad, los problemas introducidos por estos nuevos operadores, aunque similares, no son exactamente los mismos que los que caracterizaban las posiciones de poder de mercado estáticas y de lento desarrollo del s. XIX y principios del XX (ferrocarriles, azúcar, petróleo, etc.). Bien al contrario, reúnen notas distintas y se producen en un ecosistema también diferente, elementos que aconsejan que el tratamiento por parte de la Administración sea distinto.

Algunas de las circunstancias que diferencian a estos actores de las empresas dominantes de siglos anteriores radican en que, mientras las operaciones económicas de las empresas dominantes en mercados más tradicionales se centraban en un único mercado bien definido, la mayor parte de operadores dominantes actualmente (aunque siempre hay que tener presente los diferentes modelos de negocio que se han ido desarrollando en el contexto digital) pueden considerarse mercados o plataformas de dos o varios lados y operan en varios mercados a la vez generando complejos e interdependientes ecosistemas.

Respecto del primero de los rasgos, se pueden encontrar oferentes y demandantes del producto o servicio que se presenta o visibiliza en la plataforma, como si de un mercado al uso se tratase. Ésta, en su vertiente de escaparate, permite que oferta y demanda se encuentren de forma más eficiente. Estos operadores a ambos lados del mercado utilizan la plataforma como intermediadora. Pero, además, esta última participa en otro mercado, el de la publicidad, donde proporciona a terceras empresas interesadas en promocionar sus productos y servicios los grandes paquetes de datos procesados (los conocidos como *big data*) que ha ido recabando en su papel de gestor de la plataforma de intercambio en este primer mercado a cambio de una contraprestación, para que puedan afinar o perfilar la publicidad personalizada que llevan a cabo.

A mayor abundamiento, y esta circunstancia no se debe ignorar, las plataformas se han desarrollado en muchos casos también hacia una amplia diversificación de su actividad económica y su cartera de mercados, contribuyendo a difuminar las fronteras entre mercados e industrias tradicionalmente utilizados. Así, en algunas ocasiones, además de ser intermediarias y suministradoras de datos, en ocasiones, algo que está planteando importantes problemas en la introducción de *best price clauses (MFN)*, de *margin squeeze* (pinzamiento de márgenes) y de discriminación de competidores (*self-preferencing*), también participan o se integran en mercados aguas arriba o aguas abajo,

[1] Véase, entre otras, la decisión Epic games v. Apple (Case No. 4:20-cv-05640-YGR), 2021.

compitiendo ventajosamente con aquéllos a quienes presta el servicio de intermediación y de quienes ha absorbido los datos, fenómeno al que se conoce como integración vertical[2].

Una tercera nota que caracteriza este tipo de operadores y mercados es la fuerte dependencia que existe de la conocida *big data*[3], potenciada, probablemente, por el auge del IoT (el internet de las cosas), que incrementa la eficiencia en el funcionamiento, pero, a la vez, como arma de doble filo, permite aprovechar su titularidad y control para elevar las barreras de entrada, volviendo extremadamente compleja la competencia en todos mercados, afectando no sólo en el de intermediación, sino también en el de venta o suministro de productos y, por supuesto, en el de venta de *big data* en el mercado de publicidad, tendiendo hacia el dominio de los mercados[4]. Esta circunstancia, facilita la extensión del poder de mercado[5] (*leverage*[6]) que se ostenta en un área concreta a otras parcelas u otros mercados e, incluso, la incentiva, porque la complementariedad de los datos que se obtienen en mercados distintos mejora la experiencia de los productos que se ofrecen (big data es importante no sólo respecto de la cantidad de datos que se obtienen y gestionan, sino también respecto de su variedad).

La actuación como *gatekeepers* de mercados les proporciona, igualmente, un poder de mercado holgado (a veces como simple operador no evitable, otras como operador dominante pero, en cualquier caso, adjudicándoles la "especial responsabilidad") a los efectos de extender o incrementar su situación ventajosa. Este poder se ejerce en la medida en la que ocupan una posición central en la vigilancia y control del acceso de otros operadores potencialmente competidores a los mercados generando el efecto conocido como "cuello de botella": tanto al mercado de distribución, en el que ellos

[2] Modelo de negocio que se analiza por la actual presidenta de la FTC en su trabajo KHAN, L., "Amazon's Antitrust Paradox", *The Yale Journal*, 2017, n.126, págs. 710- 805.

[3] JACOBIDES, M.G., BRUNCKO, M., LANGEN, R., "Regulating Big Tech in Europe: Why, so What, and How Understanding Their Business Models and Ecosystems Can Make a Difference", 2020, págs. 1-42, pág. 15 ss. Se trata de una explotación de datos como modelo de negocio dirigido a entender mejor los patrones de conducta de los consumidores: qué es lo que estimula su satisfacción e incrementa la posibilidad de que queden bloqueados. Es la fuente principal del éxito de las big tech.

[4] PRUFER, J., SCHOTTMÜLLER, C., "Competing with Big Data", *TILEC Discussion Paper No. 2017-006*, 2017, págs. 1-50.

[5] Esta extensión de la dominancia de uno a otro mercado se produce cuando una empresa dominante utiliza el poder que ostenta en un mercado para cerrar, impedir o dificultar el acceso de competidores a un segundo mercado, algo que puede producirse fácilmente en los supuestos de mercado vinculados o donde existe integración vertical.

[6] JACOBIDES, M.G., "What Drives and Defines Digital Platform Power? A framework, with an illustration of App dynamics in the Apple Ecosystem", 2021, págs. 1-57, pág. 9. La probabilidad de la extensión del poder a otros mercados depende, entre otras, de en qué medida se encuentran los usuarios bloqueados en un determinado ecosistema porque sea extremadamente complicado o costoso cambiar de proveedor, por ejemplo, por falta de estandarización o multi-homing.

intermedian, como al mercado de publicidad. No se trata, por lo tanto, de un operador dominante más. Este papel que tienen de guardianes o vigilantes de los mercados les permite más fácilmente extender su posición de dominio a sectores colindantes.

Adicionalmente, los mercados digitales, característica también predicable de otros, como los tecnológicos, evolucionan muy rápidamente[7]. Pueden calificarse de mercados líquidos, probablemente debido a la intangibilidad de los productos o servicios que ofrecen, pero también a la escalabilidad[8] de determinados recursos (propiedad inmaterial, big data, etc.), que determina que se puede incrementar el valor y reducir el coste de forma que los mercados tienden al monopolio. La velocidad en los cambios se produce tanto en materia de crecimiento de los operadores[9], expansión o extensión a mercados colindantes (verticales y horizontales[10]) e, incluso, alteración de comportamientos estratégicos en los mismos.

Finalmente, y aunque no ha resultado una lista exhaustiva dado que cada una de las plataformas cuenta sus propias particularidades funcionales[11], que deberían tenerse en cuenta a la hora de desarrollar una regulación[12], y está inserta en distintos

---

[7] JACOBIDES, M.G., LIANOS, I., "Regulating platforms and ecosystems: an introduction", Industrial and Corporate Change, 2021, 00, 1-12, pag. 2, por ejemplo, apuntan que en la primera parte de los años 2000, se produjo uno de los cambios más bruscos en la naturaleza de las industrias y los mercados. Proliferaron muy distintas fórmulas en relación a cómo las empresas adicionan y captan el valor y se originaron una multitud de nuevos modelos. En este contexto, las arquitecturas de los mercados se volvieron más moldeables o maleables y los sectores ya no se movían al unísono, incluso desdibujando las iniciales fronteras claras que existían entre mercados o industrias.

[8] JACOBIDES, M.G., "What Drives and Defines Digital Platform Power? A framework, with an illustration of App dynamics in the Apple Ecosystem", op.cit, pág. 8.

[9] JACOBIDES, M.G., LIANOS, I., "Regulating platforms and ecosystems: an introduction", op.cit., pág. 3. Se han producido cambios dramáticos en los ecosistemas. Desde 2016, las empresas líder en Occidente son tecnológicas y, concretamente, han hecho un uso agresivo de las plataformas. Lo más reseñable no es sólo que han desplazado a líderes tradicionales, sino que han cimentado sus posiciones y crecimiento de forma extremadamente veloz.

[10] PARKER, G., "Digital Platforms and Antitrust", en prensa en Oxford *Handbook of Transnational Economic Governance*, editado opr Eric Brousseau and Jean-Michel Glachant, 2020, págs. 1-27, pág. 6. El autor explica cómo algunas de las plataformas más conocidas evolucionan y pasan de mercados digitales a físicos o de simples intermediadores a productores de películas y series de televisión.

[11] Pueden distinguirse modelos de plataforma que operan conforme a unos principios más o menos comunes, como, por ejemplo: aquéllas que funcionan como plataformas que se financian a través de publicidad (Google, Facebook, Bing, etc.), plataformas de transacción o de casación de oferta y demanda, verdaderos *marketplaces* donde se producen los intercambios (Amazon, Uber, Airbnb…) y aquellas plataformas de sistemas operativos (iOS, Appstore, Android, etc.). Las diferencias entre los distintos modelos son relevantes en la medida en la que la Administración ha de tener en cuenta los problemas en cada uno de los subsectores a la hora de analizar la conducta anticompetitiva o desarrollar regulación que no introduzca aún más distorsiones.

[12] CAFFARRA, C., ETRO, F., LATHAM, O., SCOTT MORTON, F., "Designing regulation for digital platforms: Why economists need to work on business models", 2020, https://voxeu.org/article/designing-regulation-digital-platforms. Subrayando la relevancia de

ecosistemas[13], puede denominarse a estos nuevos mercados digitales como "*winner takes all*" o "*winner takes most*". Se trata de una consecuencia económica derivada de los efectos de red, que aparecen en los mercados de dos lados, donde los sucesos que se producen a un lado de la plataforma tienen una repercusión (normalmente positiva, aunque no necesariamente) en lo que acaece al otro lado de la plataforma. Este tipo de efectos son o pueden ser de dos tipos: efectos directos e indirectos.

Como consecuencia de las características anteriores, se ha producido una situación en la que determinados operadores están experimentando un crecimiento imparable, los tentáculos de los cuales se extienden no sólo hacia los mercados en los que iniciaron sus andaduras, sino que se han diversificado, extendido, monopolizando asimismo mercados vecinos o adyacentes.

La configuración actual de los mercados digitales, sin embargo, no es un resultado inevitable ni es caprichoso o casual. Si bien determinados autores de corte más optimista han asumido que el resultado arrojado por los mercados digitales es consecuencia de un comportamiento superior o más eficiente[14] (una vez la competencia inter-plataformas ha terminado, arrojando al merecido vencedor), en realidad, ésta no parece ser toda la explicación[15] o, siquiera, siempre cierto[16] donde tienen un impacto reseñable los efectos de red e, incluso, el bloqueo de los clientes[17].

En cambio, se trata de una consecuencia de la (in)aplicación mundial de una serie de políticas con objetivos de liberalización y desregulación. La falta de control, de intervención pública suficiente y de ejercicio del poder sancionador disuasor que atajara los problemas estructurales ha llevado precisamente a este resultado. Precisamente

---

entender los modelos de los distintos operadores. Su mala comprensión se apunta como elemento central del fallo de la regulación en la solución de los problemas que plantean.

[13] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", 2019, págs. 1-133, pág. 30 y 34. Los autores definen los ecosistemas como un entramado de servicios, algunos complementarios, conectados entre ellos a través de APIs, que son accesibles sólo a servicios del mismo ecosistema.

[14] JACOBIDES, M.G., BRUNCKO, M., LANGEN, R., "Regulating Big Tech in Europe: Why, so What, and How Understanding Their Business Models and Ecosystems Can Make a Difference", op.cit., pág. 9.

[15] BAMBERGER, K.A., LOBEL, O., "Platform market power", *Berkeley technology law journal*, Vol. 32, 2017, págs. 1051-1092, pág. 1062.

[16] MOTTA, M., PEITZ, M., "Intervention triggers and underlying theories of harm. Expert advice for the Impact Assessment of a New Competition Tool", 2020, págs. 1- 63, pág. 14. Los autores sostienen que la afirmación de que más consumidores opten por una empresa determinada prueba la mejor calidad del producto no es necesariamente correcta. Por ejemplo, impidiendo a un rival acceder a una base de usuarios suficientemente amplia, se puede hacer para los consumidores la oferta del rival menos atractiva, pero esto significa necesariamente que el producto del competidor sea mejor. Quizás, sólo ha tenido acceso más pronto o tempranamente a big data (first mover advantage).

[17] JACOBIDES, M.G., "What Drives and Defines Digital Platform Power? A framework, with an illustration of App dynamics in the Apple Ecosystem", 2021, págs. 1-57, pág. 7.

para intentar, sino resolver, al menos sí paliar los efectos nocivos de las mismas, este artículo va a presentar sucintamente cuáles son las ventajas o fortalezas que pueden aportar las distintas herramientas del Derecho administrativo (sancionador).

II. TRATAMIENTO JURÍDICO DE LA SITUACIÓN

El contexto económico expuesto que afecta a determinados sectores en relación con la adquisición de un poder de mercado que difícilmente va a ser arrebatado por otros operadores, independientemente de que éstos puedan ofrecer mejores productos o servicios que los incumbentes, hace necesario plantearse si el tratamiento de estas situaciones, las conductas abusivas que desarrollen (especialmente en Europa) teniendo en cuenta muy especialmente las características estructurales del mercado, ha de ser esencialmente el mismo al que se recurrió para tratar de paliar los grandes monopolios que originaron el surgimiento del moderno Derecho antitrust en USA.

Por fortuna, actualmente tenemos muchos más instrumentos para prevenir, evitar, detectar y sancionar las conductas anticompetitivas y éstos funcionan más eficientemente porque para la Administración el uso del *big data* ya no es un fenómeno ajeno, sino que lo ha implementado en sus procedimientos de investigación.

Simplificando mucho el esquema, se puede optar entre tres herramientas distintas, que persiguen objetivos perfectamente complementarios: en primer lugar, el Derecho de la competencia tradicional contra las conductas ineficientes. Se trata de una herramienta de control *ex post* que actúa una vez la conducta ya se ha producido y su objetivo es la sanción de ésta (esencialmente centrándose en sancionar los acuerdos colusorios y abuso de posición de dominio).

En segundo lugar, puede acudirse al conocido como Derecho de la competencia regulatorio. Este tipo de medidas son propias del Derecho *antitrust* pero su aplicación se centra en la estructura del mercado e, incluso, persigue fines más amplios que el Derecho de la competencia, dirigidos a solucionar o resolver fallos de mercado. Así, por ejemplo, podemos encontrar dos tipos de medidas relativas a este campo, la primera, el control de concentraciones se aplica, a diferencia de lo que sucede con las anteriores, *ex ante*. Por lo que se puede afirmar que la intervención es más pro-activa, en comparación con el modelo reactivo de Derecho de la competencia En segundo lugar, aquellos remedios, estructurales y algunos también de comportamiento, cuyo objetivo es el retorno a la situación de mercado previa a la infracción. Dentro de éstas pueden englobarse las de escisiones empresariales, ventas de activos o desinversiones, pero también la de concesión de licencias obligatorias de *essential facilities* (infraestructuras o inputs esenciales), entre otras.

Finalmente, y ya fuera del ámbito estricto del Derecho de la competencia, aunque con importantes consecuencias en los mercados, se puede acudir a la regulación. Se trata, esta última, de un instrumento de intervención pública *ex ante* de máximos y transversal, que pretende evitar la producción de conductas anticompetitivas y su objetivo está básicamente dirigido a subsanar fallos de mercado estructurales que facilitan su proliferación. En estos supuestos se suele optar por el desarrollo de normas de conducta concretas a las que han de sujetarse todos los operadores del mercado, como, por ejemplo, puede ser la prohibición de integración vertical[18].

Hasta el momento, la intervención administrativa se ha centrado en la adopción medidas de *antitrust* tradicional y regulación administrativa. Desde el Derecho de la competencia existe actualmente una ola de intervención en el mercado de las plataformas digitales, con casos liderados por autoridades de competencia europeas y norteamericanas muy activas en el sector. Adicionalmente, no hay que olvidar los movimientos legislativos que se han promulgado ya o están preparándose en Europa y USA dirigidos a regular el sector, cuyo mayor exponente en Europa es la propuesta de *Digital Markets Act* (DMA).

Lo que, en cambio, no parece haber dado tan buenos resultados y ha sido relegado en algunos supuestos (por ejemplo, dejándose fuera de la DMA), aunque es algo que se encuentra en las agendas de las autoridades de competencia, es la aproximación de Derecho de la competencia regulatorio y, en especial, los discutidos peligros que suponen las adquisiciones asesinas, o la innovación y mejora de determinados remedios.

[18] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit., pág. 67. Los autores sugieren que podría ser oportuno adoptar remedios estructurales en estos casos en los que se puede llevar a cabo una conducta abusiva consistente en self-preferencing. Así, se puede obligar a llevar a cabo una operación de desintegración de las plataformas verticalmente integradas, ya sea un desintegración legal, operacional, informacional (de datos) o de propiedad. Este tipo de medidas se han aplicado ya por reguladores en el marco de los mercados de transporte y energía (aunque no en telecomunicaciones). Para el caso de las plataformas digitales, los mismos autores sostienen que están menos claras las consecuencias positivas que pueden tener, en general, el análisis coste-beneficio de la adopción de estas medidas, especialmente si se considera que existen medidas menos gravosas para obtener los mismos fines. Esta solución de "desintegración vertical" también ha sido propuesta por otros autores. Véase PARKER, G., "Digital Platforms and Antitrust", op.cit., pág. 16. No obstante, se apuntan claramente las dificultades de implementar esta solución al poder de mercado obtenido por las plataformas: entre otras, la complejidad para hallar una clara separación entre los distintos mercados y, en segundo lugar, que la información y los datos pueden tener efectos positivos en mercados distintos, por lo que una escisión puede contribuir a reducir el valor.

2.1. Antitrust

2.1.1. *La teoría del daño*

Es sobradamente conocido que la aplicación del Derecho de la competencia depende de la exitosa elaboración de una teoría del daño. Esta exigencia demanda que la autoridad de competencia sea capaz de desarrollar una tesis donde se pueda probar que la conducta analizada es ineficiente precisamente porque produce un daño o es susceptible de producirlo.

Sin embargo, la discusión sobre qué elemento debe sufrir el daño se encuentra actualmente abierta. La norma no cierra una única teoría del daño y, aunque es cierto que está ampliamente admitida y adoptada la teoría o estándar acuñado por el magistrado Bork en 1978 del "daño al bienestar del consumidor" (*consumer welfare standard*), esta aproximación no es inmutable.

El daño al bienestar del consumidor es un parámetro que cuadra perfectamente con los postulados de la hegemónica escuela de Chicago, donde se hace un especial hincapié en los efectos sobre las conductas en el último eslabón de la cadena de valor, los consumidores[19]. Pero, además, el daño que es susceptible de valorarse como ineficiente se analiza desde una perspectiva algo restringida, pues se prioriza el daño cortoplacista en precios, dejando de lado, no sólo el daño que se puede producir en otros operadores del mercado como proveedores, trabajadores, etc., sino que se produzca en cuestiones distintas en precios o, incluso en un momento distinto del corto plazo originándose parcelas de inaplicación del Derecho.

Este paradigma, pieza angular y determinante de la calificación final de la conducta como ilícita o pro-competitiva, sin embargo, no parece óptimo para detectar según que prácticas en mercados donde, por ejemplo, los precios pueden no ser un parámetro relevante (por ejemplo, ha permitido presuntamente crecer a golpe de precio peligrosa, sino totalmente, predatorio, a ciertas empresas como Amazon[20], pero también otros gigantes digitales[21], como pueda ser Uber[22]), que caerían por debajo del radar y

[19] KHAN, L., "Amazon's Antitrust Paradox", *op.cit.*

[20] Íbidem, obteniendo los ingresos, según la autora, de dos fuentes distintas: subsidios cruzados de otros productos que ofrece con los que sí se obtienen beneficios y utilizando los recursos de sus inversores para financiar pérdidas a corto plazo. Aunque ésta ha sido una postura fuertemente discutida por otros autores. Véase, en este sentido, STOUT, K., STAPP, A., "Is Amazon guilty of predatory pricing?", 2019. Aunque como presidenta actual de la FTC ha sostenido esta tesis en la acción presentada ante tribunales contra Amazon. BUSH, D., "What's Behind Amazon's Demand that FTC Chair Lina Khan Recuse Herself?", 2021, https://promarket.org/2021/08/24/amazon-demand-ftc-lina-khan-recusal/.

[21] Ciertos autores sostienen que, aunque es probable que se esté llevando a cabo esta estrategia en mercados digitales, las aproximaciones aplicadas hasta el momento no son apropiadas para

quedarían sin sancionar al no producir un daño directo en el consumidor en el sentido de un aumento de precios (al menos a corto plazo) o, directamente, podría derivar en considerar la situación actual como problemática[23].

Una posible vía alternativa para englobar y captar todos o, al menos, más daños sería la de sustituir el paradigma y remplazar el estándar tradicional por el de daño a la estructura del mercado[24], o, como también se ha sugerido, el de protección del proceso competitivo, de un corte más ordoliberal y más próximo al Derecho de la competencia originario europeo y regulatorio, que centrara la preocupación en los problemas de estructura de mercado en lugar de poner el foco de atención sobre el consumidor final, o, incluso, la aplicación del principio del bienestar del consumidor, pero aplicado con una perspectiva distinta[25]. La adopción de éste en ningún caso dejaría desprotegido al consumidor, más bien al contrario: quedaría protegido en la medida en la que el mercado, funcionando como un mecanismo bien engranado, puede autocorregirse en muchas ocasiones, y no sólo lo hace en materia de precios, sino en cualquier elemento que sea valorado por los consumidores (véase, por ejemplo, cuestiones de privacidad, de mayor variedad en la oferta, más innovación, etc.), sin limitar su interés a los precios.

2.1.2. *La efectividad de la aplicación del Derecho de la competencia: estándar de prueba e intervención ex post*

Incluso resolviendo la cuestión relativa al estándar o teoría de daño a adoptar, se genera un problema ulterior y es que la intervención del Derecho de la competencia se

detectarlo y sancionarlo porque, al menos en Europa, cuando estas conductas se adoptan por distintos operadores, éstos no ostentan aún una posición de poder de mercado. Adicionalmente se mantiene que el análisis de precios necesario para aplicar esta prohibición debería tener en cuenta factores distintos a la existencia de precios por debajo de coste y su recuperación en una segunda fase. Ambos lados del mercado de la plataforma han de ser tenidos en cuenta a la hora de llevar a cabo el análisis coste-beneficio. Sin embargo, el recurso a subsidios cruzados y los efectos en las estrategias de precios cuando existe competencia asimétrica son factores importantes. KASMI, S., "Predatory Pricing in Platform markets", MASTER THESIS LAW AND TECHNOLOGY JUNE 2020.

[22] BAMBERGER, K.A., LOBEL, O., "Platform market power", *op.cit*, pág.1053.

[23] JACOBIDES, M.G., LIANOS, I., "Regulating platforms and ecosystems: an introduction", op.cit., pág. 5.

[24] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit., pág. 40, donde los autores sostienen que el TJUE, especialmente en casos relativos a abusos de posición de dominio, ha entendido que la prohibición no sólo se dirige a prácticas que causan daño directo a los consumidores, sino también a aquéllas que los infligen a través del impacto sobre una estructura competitiva efectiva. Sin embargo, también reconocen los propios autores que, desde la segunda mitad de 1980, el derecho europeo de la competencia se ha caracterizado por la búsqueda de vínculos plausibles entre los efectos negativos entre la competencia en sí misma y el daño a los consumidores, esto es, en concretar lo que se conoce como teorías del daño.

[25] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit., págs. 40 ss.

produce inherente o naturalmente *ex post* o, lo que es lo mismo, tras la conducta, cuando el daño ya se ha infligido. Si bien es cierto que teóricamente se admite la intervención con la mera potencialidad de que la conducta produzca un daño, en pocas ocasiones ésta no lo causa, aunque en realidad se puede intervenir con la mera posibilidad de que la conducta produzca un daño. Adicionalmente, parece difícil, al menos en estos mercados, retornar a la situación de origen una vez la monopolización (o, desde la perspectiva del Derecho europeo, una vez la práctica excluyente) ya se ha producido. En estos supuestos el daño es difícilmente reversible, sobre todo con las sanciones habituales de imposición de multas y remedios de comportamiento.

A mayor abundamiento, y esto parece inevitable desde una perspectiva procesal y de garantías de la empresa investigada, el estándar de prueba de las autoridades de competencia es cuasi-penal y se han de cumplir las garantías procesales y sustantivas que se otorga al investigado para procedimientos penales, dado que al procedimiento administrativo sancionador se le aplican los mismos principios que al penal. Esta aproximación, por tuitiva que sea para la empresa, parece poco útil, puesto que conlleva la existencia de unos procedimientos extremadamente largos que, en mercados tan cambiantes, no pueden llegar a solucionar el problema. La razón parece clara: cuando llega la decisión, la práctica ya ha evolucionado y se aplican sanciones y remedios desarrollados para un contexto distinto y pasado del que actualmente existe.

De hecho, parece tan evidente los problemas que supone esta aproximación que la Comisión ya ha anunciado que va a adoptar un *precautionary approach* centrado en fomentar las medidas cautelares y en la adopción de una inversión de la carga de la prueba en determinadas circunstancias, esto es, obligando a las empresas a probar la eficiencia o pro-competitividad de la conducta y virando hacia una clara aplicación regulatoria del Derecho de la competencia[26].

Adicionalmente, se ha impulsado lo que se conoce como "el new competition tool" (nueva herramienta de Derecho de la competencia), que viene a solucionar parte de los problemas anunciados y que ha de aplicarse de forma complementaria al derecho antitrust para resolver los problemas a los que éste no llega y están particularmente orientados hacia los mercados digitales[27]: se trata de corregir los defectos de los

[26] PORTUESE, A., "European Competition Enforcement and the Digital Economy: The Birthplace of Precautionary Antitrust ", *Report on the Digital Economy*, 2021.

[27] SCHWEITZER, H., "The new competition tool: its institutional set-up and procedural design", 2020, págs. 1-57, pág. 10 o en mercados que no funcionan correctamente por razones ajenas a la conducta de las empresas, pero que, quizás, se aprovecha por éstas, como por ejemplo aquéllos en los que existen economías de escala, efectos de red directos o indirectos, costes de cambio de proveedor, captura del cliente o consumidor, sesgos de los consumidores. MOTTA, M., PEITZ, M., "Intervention triggers and underlying theories of harm. Expert advice for the Impact Assessment of a New Competition Tool", op.cit, pág. 7 ss.

mercados y proteger e, incluso, mejorar la competencia independientemente de la conducta analizada. En este sentido, se puede entender como un instrumento a caballo entre los instrumentos que existen en Derecho de la competencia y la regulación económica. Adicionalmente, y de forma similar a como actúa la regulación, se trata de procedimientos de naturaleza no criminal o penal, sino simplemente administrativa. Y, finalmente, se trata de medidas que permiten una intervención rápida[28] y que hacen innecesaria la definición de mercado relevante, que es otra de las cuestiones más problemáticas en los mercados digitales.

2.1.3. *Definición del mercado relevante y poder de mercado*

Aunque se trata de un paso tradicional central en la aplicación del Derecho sancionador de la competencia, se trata de un ejercicio extremadamente complejo e incierto, no sólo en mercados digitales, pero sí presenta problemas complejos de resolver si se aplica desde una perspectiva ortodoxa teniendo en consideración los precios (por ejemplo, el SSNIP test o test del monopolista hipotético), algo que no es central en algunos mercados digitales[29] donde incluso hay un problema de "precio cero"[30]. Ya ha expuesto alguna de las dificultades conceptuales que la definición tradicional de mercado relevante presenta en un contexto caracterizado por externalidades de red particularmente fuertes, ofertas a precio cero, estrategias empresariales basadas en la construcción y expansión de ecosistemas, la consideración como mercados multilaterales y ambientes dinámicos y que cambian rápidamente[31].

En mercados con estas características, distintos de los tradicionales, normalmente la definición de mercado arroja resultados cuestionables y ambiguos[32]. Adicionalmente, el problema se acrecenté cuando la intervención del derecho de la competencia no busca sancionar comportamientos pasados, sino preservar la competencia en el futuro. En

[28] SCHWEITZER, H., "The new competition tool: its institutional set-up and procedural design", 2020, págs. 1-57, pág. 5.

[29] PARKER, G., "Digital Platforms and Antitrust", op.cit, pág. 4, SAUTER, W., "A duty of care to prevent online exploitation of consumers? Digital dominance and special responsibility in EU competition law", *Journal of Antitrust Enforcement*, nº 8, 2020, págs. 406-427, pág. 413. Donde apunta que hay autores que, debido a estas complicaciones apuntan a la necesidad de entender que el abuso en sí mismo puede ser ya una prueba decisiva de la existencia de una posición de dominio, sustituyendo la necesidad de definir previamente el mercado. El mismo autor apunta también a la posibilidad de declarar la existencia de una posición de dominio basada exclusivamente en el control de los datos.

[30] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit, págs. 43 ss.

[31] íbidem, pág. 42-48, FLETCHER, A., "Market Investigations for Digital Platforms: Panacea or Complements?", *ccp-paper*, 2020, págs. 1-19, pág. 6.

[32] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit., pág. 3. ,

estos mercados caracterizados por una fuerte innovación, la percepción que tienen los consumidores de posibles sustitutos cambia muy rápidamente[33]. Se trata, en definitiva, de mercados relativamente nuevos de los que las autoridades de competencia aún están aprendiendo cómo realmente funcionan, por lo que una definición es inherentemente complicada.

Los reguladores también han puesto sobre el tapete algunas cuestiones referidas a la eficacia de las herramientas de Derecho de la competencia, que definen el mercado de forma muy restringida, de mercado en mercado, y que, por lo tanto, son ciegas al ejercicio de poder de mercado que se hace por parte de las plataformas explotando el poder en distintos mercados[34]. Estos ecosistemas en los que operan las plataformas y construidos por ellas pueden ser considerados como comunidades de empresas que, colectivamente para producir bienes. La producción se caracteriza por complementariedades que requieren la colaboración y el funcionamiento conjunto para producir valor. A medida que los operadores de estas comunidades basan su negocio en las interacciones, el poder puede surgir tanto en la dominancia como en los vínculos entre estos mercados[35].

Como consecuencia de los obstáculos en la definición de mercado relevante surge un problema adicional relativa a la determinación de la existencia de una posición de poder de mercado. La realidad es que las legislaciones de competencia están orientadas para un tipo de empresa en concreto, la cual fue causa de su origen: grandes monopolios de manufacturación[36]. Esta aproximación presenta claros problemas de adaptación a los nuevos mercados digitales porque parten de la definición del mercado en el que se ostenta una cuota determinada y tienden a darle una importancia secundaria a las barreras de entrada, cuyo efecto es incrementado por las ventajas al primero en entrar, costes de portabilidad, efectos de red (directos y, especialmente, indirectos), etc., centrales en mercados de plataformas.

2.2. Regulación

La aproximación regulatoria ha sido observada tradicionalmente por la doctrina de Derecho de la competencia con cierta desconfianza. Así, se apunta la existencia de ciertos riesgos como la posible captura del legislador y el eventual freno a la innovación

[33] SCHWEITZER, H., "The new competition tool: its institutional set-up and procedural design", op.cit, pág. 24.

[34] KHAN, L., "Amazon's Antitrust Paradox", op.cit.

[35] JACOBIDES, M.G., "What Drives and Defines Digital Platform Power? A framework, with an illustration of App dynamics in the Apple Ecosystem", op.cit., pág. 5.

[36] BAMBERGER, K.A., LOBEL, O., "Platform market power", *op.cit.*, pág. 1062.

que genera. No obstante, lo cierto es que ya desde 2020, la Comisión, en su Estrategia Digital, ya había indicado que su objetivo era el de evaluar y revisar los mercados digitales y explorar la conveniencia de incorporar reglas ex ante para asegurar que este tipo de mercados caracterizados por estar operados por grandes plataformas con poder de mercado significativo, entre otros, debido a los notables efectos de red presentes en las mismas y que actúan como guardianes del mercado, mantuvieran un funcionamiento equitativo leal y contestable para los innovadores, las empresas y los nuevos entrantes[37].

2.2.1. *El freno a la innovación*

Sostener, en términos generales, que la desregulación fomenta la innovación mientras que la intervención tiene la consecuencia inversa es sencillamente una falacia[38]. Parece claro que los mercados digitales, sin intervención administrativa, han arrojado una estructura de mercado que se encuentra lejos de poder calificarse como competitiva. Y lo han hecho por una combinación de dos factores. En primer lugar, por la superioridad en la eficiencia de los operadores en algunos casos. Pero en otros se ha logrado por conductas anticompetitivas facilitadas por el funcionamiento del mercado.

Habiéndose identificado los fallos de mercado estructurales, parece que tiene sentido intentar corregirlos a través de normas que afecten transversalmente a un tipo de operadores: los *gatekeepers* o guardianes de los mercados. En este sentido, recientemente se han adoptado en Europa algunas medidas, a nivel nacional y europeo en esta dirección. Por ejemplo, la reforma de la Ley alemana o la propuesta de *Digital Markets Act* (DMA) y otros ejemplos al otro lado del Atlántico como la Competition and Antitrust Law enforcement Act (the Klobuchar Bill)[39].

En lo relativo a esta segunda, la DMA contiene una serie de medidas que se han pensado como complementarias a la intervención *antitrust* y se han calificado como

[37] ALEXIADIS, P., DE STREEL, A., "Designing an EU Intervention Standard for Digital Platforms", *RSCAS 2020/14 Robert Schuman Centre for Advanced Studies Florence School of Regulation*, 2020, págs. 1-59, pág. 1.

[38] Aunque se pueden encontrar numerosos ejemplos que transmiten que históricamente se puede apreciar que regulaciones "invasivas" imponen costes relevantes y consecuencias a las plataformas digitales y los mercados, algo que, según los autores, aumentaría las ventajas de auto-regulación. CUSUMANO, M.A., GAWER, A., YOFFIE, D.B., "Can Self-Regulation Save Digital Platforms?", http://questromworld.bu.edu/platformstrategy/files/2021/07/PlatStrat2021_paper_38.pdf, págs. 1-32, pág. 18.

[39] Donde se sugieren medidas como la rebaja de los estándares para poder bloquear concentraciones y alteraciones de la carga de la prueba (las concentraciones propuestas deberán probarse pro-competitivas por quienes las sugieren).

insuficientes por parte de la doctrina[40], aunque pueden ir cambiando respecto del resultado final del Reglamento[41]. La filosofía general de la norma no es la de contentarse con la existencia de monopolios en los mercados digitales, obligándoles a llevar a cabo una serie de conductas, sino que adopta una aproximación mucho más ambiciosa: se trata de medidas dirigidas a fomentar la creación de competencia y de evitar la creación de monopolios en un estadio previo y preventivo[42] otorgándose especiales responsabilidades adicionales a aquellas empresas que cumplan los requisitos previstos (en relación con el volumen de negocios anual, cuando se proporcione un servicio básico de plataforma con un número mínimo de usuarios activos, y cuya posición sea duradera).

Las medidas propuestas son el resultado del aprendizaje de la aplicación antitrust previa evitando el conocido problema de *too small to succeed* y fomentar la entrada y desarrollo de operadores en los mercados, evitando que determinadas posiciones de poder se extiendan. Es decir, se han detectado cuáles son las conductas que generalmente pueden calificarse como anticompetitivas y se han reformulado en una versión regulatoria *ex ante*. Es a estos *gatekeepers* (determinados cuantitativamente, aunque también existe la posibilidad de determinarlos a través de una investigación de mercado) a los que se impone un listado de obligaciones. Esta lista, no obstante, se ha entendido como problemática por parte de la doctrina por no ser sistemática ni tener en cuenta las diferencias entre los distintos modelos de mercado de las plataformas[43].

Finalmente, y en el mismo sentido se encuentra la reforma de la legislación alemana, en línea con las soluciones aportadas por el Reglamento P2B[44] y por la CMA en el concento de guardián del mercado[45], se ha intentado resolver el problema de dependencia económica. Existen problemas en la aplicación del Derecho antitrust a situaciones en las que existe un claro abuso por parte del operador digital que, sin embargo, no ostenta una posición dominante de forma absoluta en el mercado, sino que

---

[40] CAFFARRA, C, SCOTT MORTON, F., "The European Commission Digital Markets Act: A translation".

[41] VELASCO SAN PEDRO, L.A., "El papel del derecho de la competencia en la era digital", *Revista de Estudios Europeos, n 78, 2021,* Págs. 93-110. El autor entiende que es necesario que el Reglamento que finalmente se adopte habría de perfeccionarse al menos en las conexisiones de la aplicación pública-privada y a aplicación privada de las disposiciones del futuro reglamento.

[42] JACOBIDES, M.G., "What Drives and Defines Digital Platform Power? A framework, with an illustration of App dynamics in the Apple Ecosystem", op.cit, pág. 6.

[43] CAFFARRA, C, SCOTT MORTON, F., "The European Commission Digital Markets Act: A translation".

[44] REGLAMENTO (UE) 2019/1150 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de junio de 2019 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.

[45] ALEXIADIS, P., DE STREEL, A., "Designing an EU Intervention Standard for Digital Platforms", *RSCAS 2020/14 Robert Schuman Centre for Advanced Studies Florence School of Regulation*, 2020, págs. 1-59, pág. 7 ss.

su poder es relativo respecto de algunos operadores, porque, por ejemplo, puede ser un operador que no puede evitarse. En estos casos, el derecho europeo de la competencia tiene pocas opciones porque falta uno de los requisitos, el de dominancia absoluta o poder de mercado absoluto. Como los problemas de dependencia son centrales en este tipo de mercados, se ha optado por una vía de refuerzo de las facultades administrativas para estos supuestos.

2.2.2. *Fortalezas de la regulación*

En cualquier caso, tratar los problemas con herramientas regulatorias, esto es, ordenando o prohibiendo conductas en general, de forma transversal y *ex ante*, presenta unas ventajas innegables. En primer lugar, porque no siempre la posición de dominio es absoluta en el mercado. La necesidad de acudir a medidas alternativas al Derecho de la competencia ante este problema es distinta en USA y en Europa, porque en el primero, la conducta sancionada es la obtención de poder de mercado (monopolización), partiendo de que es posible que quien lleva a cabo tales acciones no ostenta aun la misma. En Europa, sin embargo, hay una constricción adicional, la de que no puede aplicarse el Derecho a las prácticas que lleve a cabo una empresa que aún no se encuentre en posición de dominio absoluta. Si la causa del poder que tiene una empresa no se encuentra en razones estructurales del mercado (cuántos operadores hay y la posición de cada uno de ellos en el contexto), sino que proviene de razones distintas, no se puede acudir al Derecho de la competencia, sino a instrumentos propios de la competencia desleal. Éstos son herramientas de Derecho privado de daños, que obligan a los perjudicados por la conducta a interponer acciones con los obstáculos propios de esta rama del Derecho.

Adicionalmente, se ha de reconocer que los daños no siempre se causan al mercado o al consumidor (en el restringido concepto que existe de daño al consumidor que es en precios y a corto plazo). Es posible que se dañen otros bienes jurídicos como la intimidad/privacidad, la transparencia, DDHH, etc. Intentar proteger de forma directa estos elementos a través del Derecho de la competencia, cuyo objetivo es el de proteger la eficiencia y la estructura competitiva del mercado contribuye a desvirtuar y distorsionar la herramienta[46]. Precisamente porque se lesionan otros bienes e intereses distintos de los protegidos por el Derecho antitrust es indispensable regular el mercado.

[46] Para una perspectiva distinta, véase ECONOMIDES, N., LIANOS, I., “Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective”, *Journal of Competition Law & Economics*, 2021, págs. 1-83 quienes entienden que la gestión de los datos, específicamente en el sector digital, plantea retos desde la perspectiva de la aplicación del Derecho de la competencia, con el que se debe evitar la explotación de datos personales y restricciones de su privacidad. Aunque reconocen que la protección de datos y el derecho de la

En tercer lugar, es necesario reconocer que, cuando el problema es estructural, esto es, la posición de dominio no se ostenta y el poder de mercado no se ejerce por comportamientos anticompetitivos en el mercado, sino que el propio funcionamiento del mercado empuja a tal situación de competencia por el mercado (barreras de entrada causadas por multitud de condiciones como los fuertes efectos de red, la relevancia del big data, etc.) la herramienta más conveniente es la regulación[47].

2.3. Derecho de la competencia regulatorio

Una de las preocupaciones centrales actuales radica en intentar salvar este ángulo muerto del Derecho de la competencia, el de las concentraciones, que han proliferado en los últimos años en los mercados digitales[48], cuando la compra o la absorción se produce sobre competidores potenciales aun en desarrollo ("nascent competitors").

Parece que especialmente en algunos mercados en los que la innovación y las cuestiones técnicas o digitales juegan un papel importante, la aproximación adoptada por las autoridades de la competencia no está tan orientada hacia precios, como sucedía tradicionalmente y se mantiene en muchos mercados, sino que está virando hacia la conocida como "innovation approach", donde las conductas se admiten dependiendo no tanto de los precios resultantes, que ha pasado a ser un factor relegado, sino de la innovación que fomentan.

No obstante, en materia de concentraciones que han de ser autorizadas por las autoridades de competencia, parece que los aplicadores no se han adaptado perfectamente a la detección de los riesgos para la innovación que presentan algunas operaciones.

El derecho de la competencia, como hemos sostenido inicialmente, debería ir dirigido a fomentar al mantenimiento y proliferación de competidores eficientes en el mercado, algo que puede entenderse como contradictorio con las concentraciones del mercado. Esta aproximación pro-mercado no necesariamente ha de impedir cualquier concentración, pero, para autorizarse, las eficiencias que arroje deberían ser considerables (por ejemplo, en el mercado digital, el acceso a datos que puedan arrojar

---

competencia adoptan dos perspectivas distintas respecto de esta circunstancia, estando el primero orientado a solucionar el fallo de mercado.

[47] ALEXIADIS, P., DE STREEL, A., "Designing an EU Intervention Standard for Digital Platforms", *RSCAS 2020/14 Robert Schuman Centre for Advanced Studies Florence School of Regulation*, 2020, págs. 1-59, págs. 17 ss.

[48] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit., pág. 110, remitiendo a un informe de la OECD, "Data-Driven Innovation: Big Data for Growth and Well-Being", Paris, 2015 y BOURREAU, M., DE STREEL, A., "Digital Conglomerates and EU Competition Policy", 2019, págs. 1-44, a disposición para consultar en 8377.pdf (crid.be), pág. 21.

mejoras si se combinan con aquéllos que ya tenía la empresa absorbente), al menos lo suficiente como para compensar la desaparición de un operador que estimula la inversión en innovación, entre otros y que, puede, además, contribuir a elevar las barreras de entrada al controlar un grupo de datos esencial y no replicable por otros competidores[49].

Es cierto, sin embargo, y éste es el problema, que no todos los competidores son iguales, en el sentido de tener el mismo efecto en el mercado: existen competidores grandes y fuertes y otros pequeños y débiles. Hasta el momento ha interesado mantener el primer grupo, precisamente porque los pequeños y débiles, en realidad, no generan el suficiente efecto pro-competitivo como para querer mantenerlos en el mercado a toda costa y puede arrojar más eficiencias que sean absorbidos.

Ahora bien, en mercados innovadores esta dicotomía ya no está tan clara. Existen numerosos supuestos de empresas muy innovadoras (por ejemplo, start-ups biotecnológicas en el mercado farmacéutico, pero también en los mercados digitales) que, pese a obtener cuotas de mercado inicialmente muy limitadas -porque se trata de empresas relativamente jóvenes- tienen un potencial de crecimiento y desarrollo fuerte. Aquí es donde puede fallar el Derecho de la competencia; cuando se trata de aplicar instrumentos tradicionales de control de concentraciones porque, en estos mercados, las absorciones suelen hacerse en fases tempranas del desarrollo, lo que hace que, desde una perspectiva de cuota de mercado, las operaciones pasen inadvertidas y, aunque no lo hagan, que los sistemas de prueba exigidos, hagan imposible prohibir la misma. Este tipo de concentraciones no necesariamente arrojarían resultados anticompetitivos, incluso en el supuesto de analizarse, por ejemplo, porque pueden producirse sinergias beneficiosas entre las empresas grandes absorbentes y las start-ups que ofrecen ideas innovadoras pero que carecen, por ejemplo, de músculo económico para poder ejecutarlas con solvencia. La cuestión es que, al no analizarse, es posible que algunas con efectos anticompetitivos, como refuerzos de dominancia, incremento de barreras de entrada, etc., sean indetectables[50].

---

[49] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., “Competition Policy for the Digital Era”, op.cit., pág. 110.

[50] Para solucionar este problema se han sugerido múltiples alternativas: desde rebajar los umbrales de análisis para aquéllos supuestos en los que la adquirente sea una dominante y existen fuertes efectos de red, reforzar el procedimiento o mecanismo de reenvío o de referencia de las autoridades nacionales a la Comisión (por ejemplo, con referencias o remisiones de la autoridad española en los supuestos de Apple y Shazam o Facebook y Whatsapp o la británica para el supuesto de Facebook e Instagram), revertir la carga de la prueba de los efectos pro-competitivos, guiarse por el precio de compra, no por los volúmenes de mercado (como han hecho Alemania y Austria), revisitar teorías del daño, notificaciones ex post, etc. Pero existen también numerosos obstáculos, entre los que se encuentra la necesaria modificación del reglamento de concentraciones, afectación a la seguridad jurídica, la eficiencia en la aplicación de los recursos de

Siendo la situación anterior ya grave en sí misma porque se elimina un operador competidor potencial en las concentraciones horizontales que podría ejercer presión en el mercado para estimular mejoras, existe un supuesto que generaría consecuencias presumiblemente más graves, de cuya existencia sólo existen pruebas en el mercado farmacéutico[51] pero que está comenzando a preocupar a la Comisión europea también en el mercado digital[52]: las adquisiciones asesinas ("killer acquisitions"). Aunque parece que se trate de una situación excepcional[53], ésta se producen cuando la empresa absorbente o compradora adquiere la start-up con una línea de investigación en desarrollo para un producto o servicio innovador y corta, al adquirir la propiedad, la inversión, evitando el efecto remplazo y manteniéndose como un dominante vago evitando los efectos pro-competitivos que podría haber tenido la concentración.

III. CONCLUSIONES

Considerando las cuestiones expuestas, parece que puede afirmarse que una aproximación tradicional exclusivamente desde la perspectiva del Derecho antitrust es insuficiente para hacer frente a los problemas que plantean estos nuevos operadores, no tanto por las conductas llevadas a cabo por los operadores de los mismos, sino por los fallos del mercado.

Es innegable los operadores que ostentan poder de mercado en estos mercados digitales han obtenido la misma parcialmente debido a su eficiencia. Ahora bien, desde una perspectiva estructural, parece también evidente la inevitabilidad de que tal cual están configurados y cuál es su estructura, los mismos admitan más de un operador (efectos de red directos e indirectos y enormes barreras de entrada generadas como consecuencia del control de infraestructuras esenciales como puedan ser los llamados *big data*).

Es necesario continuar la vigilancia y persecución de determinadas conductas, específicamente las prácticas excluyentes. Ahora bien, la aplicación del Derecho antitrust debe hacerse desde la adopción de un paradigma distinto al ampliamente aceptado hasta el momento. El bienestar del consumidor, al menos en su aplicación tradicional

---

la Administración, etc. Véanse, entre otros, EXPERT GROUP FOR THE OBSERVATORY ON THE ONLINE PLATFORM ECONOMY, "Measurement & Economic Indicators", 2021, págs. 1-39, pág. 25 ss.

[51] CUNNINGHAM, C., EDERER, F., MA, S., "Killer Acquisitions", *Journal of Political Economy,* Vol. 129, nº. 3, 2021, págs. 649-702. CUNNINGHAM, C., BENSON, A., "Killing innovation in the pharmaceutical industry", 2020, a disposición para consultar en https://www.london.edu/think/iie-killing-innovation-in-the-pharmaceutical-industry

[52] OECD, "Start-ups, killer acquisitions and merger control - Note by the European Union", 2020.

[53] CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", op.cit., pág. 117 ss.

más restrictiva centrada en precios a corto plazo, no es suficiente para capturar todas las conductas perjudiciales.

Paralelamente, y vistas las notas que caracterizan estos mercados, es indispensable poner el foco de atención sobre el medio, esto es, las estructuras que permiten y facilitan que las posiciones de dominio y las conductas abusivas proliferen. La intervención ex ante transversal tiene, no obstante, que tener en consideración las características particulares de los distintos modelos de negocio operados en los mercados digitales. Igualmente, y porque es un mercado nuevo cuyo funcionamiento aún se desconoce enteramente, al igual también se ignoran los graves problemas que puede desencadenar, parece oportuno acudir al conocido como "precautionary approach" o antitrust, algo que se ha reflejado en la propuesta de DMA. Se trata de reconocer que la situación de desconocimiento e incertidumbre exige una modificación de ciertas exigencias jurídicas como eximir de la prueba del daño actual (el daño hipotético es suficiente), invertir la carga de la prueba hacia quien más información controla, como las plataformas, entre otras medidas más novedosas como las desinversiones verticales o la obligación de compartir determinadas infraestructuras necesarias.

Finalmente, y si se adopta el paradigma de protección del mercado plural en sí mismo o buen funcionamiento del mercado, los instrumentos de antitrust regulatorio han de ser fomentados. Si la estructura y funcionamiento de los mercados en condiciones lícitas ya hace extremadamente complicada el surgimiento de competidores en el mismo, cuando éstos aparecen (aunque su proliferación se habrá de fomentar vía regulatorio) han de preservarse. Así, las concentraciones en estos mercados deberían autorizarse solo en aquellos supuestos en los que pueda probarse por la empresa solicitante que la concentración arroja unas eficiencias que son capaces de compensar sobradamente la pérdida de un competidor en el mercado. Los compromisos donde se recojan las condiciones en las que se autorice la concentración deben establecer vías para poder revertir la misma en los supuestos de finalmente resultar anticompetitiva. Adicionalmente, y con el fin de asegurar que las concentraciones son analizadas, se deben introducir medidas dirigidas evitar que operaciones relevantes pasen inadvertidas por los rígidos requisitos exigidos para aplicar la obligación de solicitar autorización. Bien sea a través de la consideración del valor de compra como parámetro, bien sea reforzando los mecanismos de referencia o reenvío a la Comisión Europea, bien sea rebajando los umbrales proporcionalmente, se ha de hacer un esfuerzo conjunto por someter al escrutinio competitivo a más operaciones.

Finalmente, y aunque no parece aún un problema acuciante en el mercado digital, las adquisiciones asesinas son una situación a la que se debe prestar atención. Independientemente de lo bajo que sea el porcentaje (en el mercado farmacéutico) con

el que se producen, sus consecuencias son extremadamente gravosas en un mercado carente de competencia.

IV. BIBLIOGRAFÍA

ALEXIADIS, P., DE STREEL, A., "Designing an EU Intervention Standard for Digital Platforms", *RSCAS 2020/14 Robert Schuman Centre for Advanced Studies Florence School of Regulation*, 2020, págs. 1-59.

BAMBERGER, K.A., LOBEL, O., "Platform market power", *Berkeley technology law journal*, Vol. 32, 2017, págs. 1051-1092.

BOURREAU, M., DE STREEL, A., "Digital Conglomerates and EU Competition Policy", 2019, págs. 1-44, a disposición para consultar en 8377.pdf (crid.be).

BUSH, D., "What's Behind Amazon's Demand that FTC Chair Lina Khan Recuse Herself?", 2021, https://promarket.org/2021/08/24/amazon-demand-ftc-lina-khan-recusal/.

CAFFARRA, C, SCOTT MORTON, F., "The European Commission Digital Markets Act: A translation", a disposición para consultar en https://voxeu.org/article/european-commission-digital-markets-act-translation.

CAFFARRA, C., ETRO, F., LATHAM, O., SCOTT MORTON, F., "Designing regulation for digital platforms: Why economists need to work on business models", 2020, https://voxeu.org/article/designing-regulation-digital-platforms.

CRÉMER, J., MONTJOYE, Y.A., SCHWEITZER, H., "Competition Policy for the Digital Era", 2019, págs. 1-133, a disposición para consulta en https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

CUNNINGHAM, C., BENSON, A., "Killing innovation in the pharmaceutical industry", 2020, a disposición para consultar en https://www.london.edu/think/iie-killing-innovation-in-the-pharmaceutical-industry.

CUNNINGHAM, C., EDERER, F., MA, S., "Killer Acquisitions", *Journal of Political Economy,* Vol. 129, nº. 3, 2021, págs. 649-702.

CUSUMANO, M.A., GAWER, A., YOFFIE, D.B., "Can Self-Regulation Save Digital Platforms?", http://questromworld.bu.edu/platformstrategy/files/2021/07/PlatStrat2021_paper_38.pdf, 2021, págs. 1- 32.

ECONOMIDES, N., LIANOS, I., "Restrictions On Privacy and Exploitation In The Digital Economy: A Market Failure Perspective", *Journal of Competition Law & Economics*, 2021, págs. 1-83.

EXPERT GROUP FOR THE OBSERVATORY ON THE ONLINE PLATFORM ECONOMY, "Measurement & Economic Indicators", 2021, págs. 1-39

FLETCHER, A., "Market Investigations for Digital Platforms: Panacea or Complements?", ccp-paper, págs. 1-19, 2020.

GOOS, M., VAN CAYSEELE, P., WILLEKENS, B., "Platform Pricing in Matching Markets", Review of Network Economics 2013; 12(4): 437-457.

JACOBIDES, M.G., "What Drives and Defines Digital Platform Power? A framework, with an illustration of App dynamics in the Apple Ecosystem", 2021, págs. 1-57, a disposición para consultar en https://events.concurrences.com/IMG/pdf/jacobides_platform_dominance.pdf.

JACOBIDES, M.G., BRUNCKO, M., LANGEN, R., "Regulating Big Tech in Europe: Why, so What, and How Understanding Their Business Models and Ecosystems Can Make a Difference", 2020, págs. 1-42, a disposición para consultar en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3765324.

JACOBIDES, M.G., LIANOS, I., "Regulating platforms and ecosystems: an introduction", Industrial and Corporate Change, 2021, 00, 1-12.

KASMI, S., "Predatory Pricing in Platform markets", MASTER THESIS LAW AND TECHNOLOGY JUNE 2020, a disposición para consultar en http://arno.uvt.nl/show.cgi?fid=152379.

KHAN, L., "Amazon's Antitrust Paradox", *The Yale Journal*, 2017, n.126, págs. 710-805.

MOTTA, M., PEITZ, M., "Intervention triggers and underlying theories of harm. Expert advice for the Impact Assessment of a New Competition Tool", 2020, págs. 1- 63, kd0420575enn.pdf (europa.eu).

OECD, "Start-ups, killer acquisitions and merger control - Note by the European Union", 2020.

PARKER, G., "Digital Platforms and Antitrust", en prensa en Oxford Handbook of Transnational Economic Governance, editado opr Eric Brousseau and Jean-Michel Glachant, 2020, págs. 1-27, a disposición para descargar en Digital Platforms and Antitrust by Geoffrey Parker, Georgios Petropoulos, Marshall W. Van Alstyne :: SSRN.

PORTUESE, A., "European Competition Enforcement and the Digital Economy: The Birthplace of Precautionary Antitrust ", *Report on the Digital Economy*, 2021, a disposición para consultar en https://gaidigitalreport.com/2020/08/25/antitrust-enforcement-activity-in-digital-markets-europe/.

PRUFER, J., SCHOTTMÜLLER, C., "Competing with Big Data", *TILEC Discussion Paper No. 2017-006*, 2017, págs. 1-50.

SAUTER, W., "A duty of care to prevent online exploitation of consumers? Digital dominance and special responsibility in EU competition law", *Journal of Antitrust Enforcement*, nº 8, 2020, págs. 406-427.

SCHWEITZER, H., "The new competition tool: its institutional set-up and procedural design", 2020, págs. 1-57, kd0420574enn.pdf (europa.eu).

STOUT, K., STAPP, A., "Is Amazon guilty of predatory pricing?", 2019, a disposición para consular en Is Amazon Guilty of Predatory Pricing? - International Center for Law & Economics (laweconcenter.org).

VELASCO SAN PEDRO, L.A., "El papel del derecho de la competencia en la era digital", *Revista de Estudios Europeos, n 78, 2021,* Págs. 93-110.

THE DIGITAL ECONOMY AND URBAN MOBILITY: A CHALLENGE FOR REGULATION FOR SOCIAL RATIONALES AND CONSUMER PROTECTION

Por

MICHAEL FEHLING, LL.M. (BERKELEY) / NICO SCHRÖTER, LL.M. (LSE)
Tenured professor at Bucerius Law School, Hamburg - Chair of Public Law III (Public Law and Comparative Law) / Research assistant at Bucerius Law School, Hamburg - Chair of Public Law III (Public Law and Comparative Law)

michael.fehling@law-school.de / nico.schroeter@law-school.de

Revista General de Derecho de los Sectores Regulados 8 (2021)

ABSTRACT: The digital economy and its services pose new regulatory challenges. By looking at the German Passenger Transportation Act (PTA) and novel ride-pooling services, the article exemplifies how existing regulatory frameworks fail to accommodate new phenomena. Focussing on social aspects and aspects of consumer protection, the article illustrates which regulatory challenges are being posed by platform-based services and how they can be met by way of regulated self-regulation.

KEYWORDS: digital economy, platform economy, urban mobility, public service, regulation, ride pooling, self-regulation, regulated self-regulation, Germany.

SUMMARY: I. Introduction. II. Regulatory goals and strategies. 2.1. The case for regulation. 2.2. Combining regulatory strategies. III. Regulating digital services in the mobility sector. 3.1. The German Passenger Transportation Act and new mobility services. 3.1.1. Fixed categories of transport services. 3.1.2. Recent reform of the Passenger Transportation Act. 3.2. Prescient planning in order to create a system of sustainable urban mobility. IV. Some general conclusions. 4.1. Challenges and regulatory approaches. 4.2. Consumer protection and the reputation systems of online platforms. 4.3. Final remarks. V. BIBLIOGRAPHY.

La economía digital y la movilidad urbana: un reto de regulación para las fundaciones sociales y la protección al consumidor

RESUMEN: La economía digital y sus servicios plantean nuevos retos normativos. Mirando a la Ley de Transporte de Pasajeros (PTA) alemana y los nuevos servicios de transporte compartido, el artículo ejemplifica cómo los marcos reguladores existentes no logran adaptarse a los nuevos fenómenos. Centrándose en los aspectos sociales y los aspectos de la protección de los consumidores, la publicación ilustra qué desafíos regulatorios plantean los servicios basados en plataformas y cómo pueden resolverse mediante la autorregulación regulada.

PALABRAS CLAVE: Economía digital, economía de plataformas, movilidad urbana, servicio público, regulación, paseo en grupo, autorregulación, autorregulación regulada, Alemania.

I. INTRODUCTION

The digital economy and its services pose new regulatory challenges. This also holds true for the so-called "sharing economy"[1] organised around digital platforms. Prominent examples, which have already been subject of ample discussion, are "Uber" for taxi-like services or "AirBnB" for short-term rentals. Other platforms such as eBay allow for the exchange of goods. Finally, social media like Facebook are another example of platform-based services.

This paper will deal with the legal problems of such digital platforms. More specifically, we will look at them from the perspective of regulatory strategies. In doing so, we will focus on social aspects. As to that, one must not only consider the user-perspective and discuss issues of consumer protection such as the right to equal and affordable access to such platforms. Rather, one should also look at the working conditions in this part of the economy. For further details we will turn to the mobility sector with a special focus on the situation in Germany. The new proposals of the European Commission for a Digital Services Act (DSA)[2] and a Digital Markets Act (DMA)[3] will only be mentioned in passing because both do not deal with social issues and only briefly touch on questions of consumer protection.

Firstly, we will try to map out some major regulatory challenges and strategies. As to that, we look at digital services in general but will place a special focus on social issues (0.). Secondly, we will take a closer look at the legal developments of the regulation of digital platforms in the mobility sector in Germany (0.). Finally, we will draw some conclusions, once again on a more general level. This shall particularly include problems of reputation systems regarding aspects of consumer protection (0.).

II. REGULATORY GOALS AND STRATEGIES

2.1. The case for regulation

According to standard economic wisdom, the most convincing reason for regulatory intervention is the danger of market failure because of - amongst others - negative external-

[1] Hereunto *Heinrichs/Grunenberg*, Sharing Economy: Auf dem Weg in eine neue Konsumkultur? (2012), https://nbn-resolving.org/urn:nbn:de:0168-ssoar-427486 (accessed 18 Oct. 2021).

[2] COM/2020/825 (final).

[3] COM/2020/842 (final).

ities or information asymmetries.[4] Especially, structural imbalances of bargaining power can constitute another form of market failure, requiring regulation for consumer protection. Evidently, these rationales for regulation can overlap. In the mobility sector, potential market failure also threatens to impair the individual's right to basic mobility [*Mobilitätsgewährleistung*], which in Germany can be derived from a participatory dimension [*Teilhabefunktion*] of basic rights in conjunction with the social state principle in Art. 20 (1) of the German Basic Law [*Grundgesetz*].[5] Therefore, economic and social rationales for regulation are closely interlinked.

1.1) First of all, there is concern that digital platforms could attain a dominant market position by utilising network effects.[6] This poses a challenge not only to competition law. However, efforts for a "level playing field" must not lead to undue obstacles for innovative services as far as they indeed operate more efficiently, offer better services and promise new job opportunities. Therefore, it is not sufficient to simply make sure that existing regulation also applies to new competitors. Instead, we need an updated regulatory framework which is sufficiently flexible to allow digital platforms to operate while ensuring adequate responses to potential market failure, including effective enforcement. As to that, the proposed Digital Markets Act might bring some relief.[7]

1.2) Consumer protection regulation to rectify information asymmetries is an even more challenging issue in the platform economy.[8] Traditional consumer protection law is based upon the assumption of "bipolar" transactional relationships between a business and a consumer. In contrast, digital platforms establish a "triangular" situation with contractual relationships between the platform and the service provider, between the platform and the user, and - of course - between the service provider and the user.[9]

---

[4] See further *Rodi*, Ökonomische Analyse des Öffentlichen Rechts (2014), pp. 32 et seqq.

[5] *Fehling*, Urbane Verkehrskonzepte der Zukunft - Ökonomische versus ordnungsrechtliche Instrumente, ZUR 2020, pp. 389 et seq.

[6] See *Busch/Schulte-Nölke/Wiewiórowska-Domagalska/Zoll*, The Rise of the Platform Economy: A New Challenge for EU Consumer Law?, EuCML 2016, p. 4; *Knieps*, Network Economics of Shared Mobilty, 20 Network Industries Quarterly (2018) pp. 9-12.

[7] See further *Gielen/Uphues*, Digital Markets Act und Digital Services Act: Regulierung von Markt- und Meinungsmacht durch die Europäische Union, EuZW 2021, pp. 627-637.

[8] See *Edelman/Geradin*, Efficiencies and Regulatory Shortcuts: How should we regulate Companies like Airbnb and Uber?, 19 Stanford Technology Law Review (2016), p. 315.

[9] Cf. T*erryn*, The Sharing Economy in Belgium - A Case for Regulation, EuCML 2016, pp. 46, 50; *Katz*, Regulating the Sharing Economy, 30 Berkeley Technology Law Journal (2015), p. 1080; *Busch/Schulte-Nölke/Wiewiórowska-Domagalska/Zoll* (2016: 4).

Very relevant information is located within the algorithms of the platform's software and is accessible neither to the service providers nor to the users. Having control over both a myriad of data and the algorithms processing them gives the platform providers enormous power to nudge the users and the service providers towards adopting a behaviour most favourable to them. For example, surge pricing in transportation services is a hotly debated issue in this context.[10] Here, one can see how, if it comes to pricing, consumer protection can overlap with social aspects of regulation since a (constitutional) mobility guarantee is effectively undermined if people with low income cannot afford the relevant services.

Last but not least, there are severe privacy concerns since digital platforms are in a position to collect much more personal data from both users and service providers than is needed to fulfil their core economic function as a means to reduce search costs and facilitating trust. One must be aware of the risk that platforms commercially use or even sell those data[11] in a similar way as companies like Facebook and Google.

1.3) The digital economy also challenges traditional labour law.[12] Some mobility platforms like MOIA in Germany employ their own drivers. Others, such as Uber, like to refer to their drivers as independent contractors. However, it is less than clear whether they might better be considered employees. The Uber-decisions of the European Court of Justice (ECJ) also point in this direction with the Court stating that Uber exercises "deci-

[10] See *Edelman/Geradin* (2016: 301-302) with further references; *Griffith*, The Uber Loophole That Protects Surge Pricing, 26 Virginia Journal of Social Policy & the Law (2019), esp. pp. 40 et seq. For Uber's surge pricing mechanisms see the company's official website: https://www.uber.com/en-DE/drive/partner-app/how-surge-works/ (accessed 18 Oct. 2021).

[11] *Katz* (2015: 1113-1114) speaks more generally of „potential for misuse".

[12] See generally *Krause*, Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0, NZA-Beilage 2017, pp. 58 et seq. For a similar assessment see the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, A European agenda for the collaborative economy, COM/2016/356 (final), p. 11. In the UK, an Employment Court and the Employment Appeal Tribunal have acknowledged the claims of Uber-drivers, recognising them as employees with rights to a minimum wage, *Davies*, Uber loses appeal in UK employment rights case, The Guardian (10 Nov. 2017), https://www.theguardian.com/technology/2017/nov/10/uber-loses-appeal-employment-rights-workers (accessed 18. Oct. 2021). A French appellate court followed that ruling in 2019, overturning an earlier judgement, *Lee*, French court follows UK in ruling against Uber in 'employment' contract case, The Telegraph (11 Jan. 2019), https://www.telegraph.co.uk/news/2019/01/11/french-court-follows-uk-ruling-against-uber-employment-contract/ (accessed 18. Oct. 2021). For U.S. court rulings, see *Katz* (2015: 1104); *DiMatteo*, Regulation of Share Economy: A Consistently Changing Environment, in: Schulze/Staudenmayer (eds.), Digital Revolution: Challenges for Contract Law in Practice (2016), pp. 96 et. seq.

sive influence" over the conditions under which the service is provided by its drivers.[13] After all, the imbalance of power might be similar to that in traditional employment relationships. As far as people must make a living by providing platform-driven services, they might need regulatory protection against an abuse of power on part of the platform operator. This for example includes the service providers' right to operate on different platforms (multi-hosting).[14]

2.2. Combining regulatory strategies

Legal scholars and regulatory theory distinguish three main modes of regulation: direct regulation by the state, self-regulation and - as a sort of hybrid - regulated self-regulation, meta-regulation, or co-regulation.

2.1) *Self-regulation*[15] by the platform providers is, up to the present day, the dominant mode of regulation in the digital economy. The platforms determine the terms and conditions of their intermediary function and set rules of behaviour both for the service providers and for their customers. Reputation systems which allow for ratings and reviews by both customers and service providers are an important tool for the self-regulation of digital platforms.[16] We will elaborate on them in more detail later.[17]

Under certain conditions, self-regulation can be a more flexible and cheaper way to address regulatory problems compared to direct regulation by the state.[18] However, self-regulation often lacks transparency and fails to account for the interests of actors other than the platforms themselves. Therefore, a purely self-regulatory approach bears the risk of further increasing the platforms' power.

---

[13] See ECJ, Judgment of the Court (Grand Chamber), 20 December 2017 - Case C-434/15 (Asociación Profesional Élite Taxi/Uber Systems Spain SL), ECLI:EU:C:2017:981; ECJ, Judgment of the Court (Grand Chamber), 10 April 2018 - Case C-320/16 (Uber France SAS/Nabil Bensalem), ECLI:EU:C:2018:221.

[14] See (also with the objective of promoting competition) the Twenty-first Biennial Report of the German Monopolies Commission in accordance with Sec. 44 (1) of the German Act against Restraints of Competition (2016), par. 1232 et seq. and 1331, English excerpt available at https://www.monopolkommission.de/images/HG21/HGXXI_Chapter_V.pdf (accessed 18. Oct. 2021). See also *Katz* (2015: 1124).

[15] See further *Coglianese/Mendelson*, Meta-Regulation and Self-Regulation, in: Baldwin/Cave/Lodge (eds.), The Oxford Handbook of Regulation (2012), pp. 146 et seqq.; *Baldwin/Cave/Lodge*, Understanding Regulation (2012), pp. 137 et seqq.

[16] See *Edelman/Geradin* (2016: 315 et seq.).

[17] Below 0.

[18] *Baldwin/Cave/Lodge* (2012: 139 et seqq.).

2.2) *Direct regulation* by the state[19] (be it on the European or on the national level) often has (especially if it is by way of command-and-control) a bad reputation if it comes to innovative and dynamic business ideas. The digital economy is often said to be ill-suited for such "top-down" regulation because the state only has limited experience with new business models and lacks reliable information on the operation (and in particular the algorithms) of such platforms.[20]

Nevertheless, direct regulation by way of command-and-control is routinely called for in order to guarantee legal certainty. Strict and stable regulation by the state is best suited to provide a regulatory level playing field. This can make direct regulation preferable if the matter is not too complex and the public interest in regulation is particularly strong.[21]

2.3) *Regulated self-regulation*, meta-regulation and co-regulation can combine the advantages of both private self-regulation and direct regulation by the state.[22] Public authorities may define certain regulatory standards or objectives to be achieved while giving the platform providers a certain scope for implementation. Within the regulatory framework, each of those elements (self- or state-regulation) might be given different weight. Therefore, the spectrum might reach from direct regulation with only a few self-regulatory elements to self-regulation with only little guidance by the state. Moreover, regulated self-regulation can be either more or less cooperative.[23]

However, combining both modes of regulation will not work if the gap between the interests involved is too large. If the regulatory protection of consumers and certain public interests is in line with the interest of the platform providers to preserve a positive image of their company, it might only take selective command-and-control-regulation to mitigate smaller conflicts. If, however, one must deal with strong and antagonistic interests - as is the case in employment law - only robust state regulation will do the job.

---

[19] See *Baldwin/Cave/Lodge* (2012: 105 et seqq.).

[20] Cf. *Finck*, Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy, 43 E.L. Rev. (2018) p. 51-52.

[21] Cf. *Baldwin/Cave/Lodge* (2012: 107).

[22] See *Baldwin/Cave/Lodge* (2012: 146 et seqq.); *Finck* (2018: 65); more generally (from a German perspective) *Eifert*, Regulierungsstrategien (§ 19), in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (eds.), Grundlagen des Verwaltungsrechts, (2nd edn. 2012), rec. 52 et seq.; for different perspectives see *Berg/Fisch/Schmitt Glaeser/ Schoch/Schulze-Fielitz (eds.),* Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Die Verwaltung, Beiheft 4, 2001.

[23] For a nuanced display see Hoffmann-Riem, Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext, in: Fehling/Schliesky (eds.), Neue Macht- und Verantwortungsstrukturen in der digitalen Welt (2016), pp. 40 et seq.

III. REGULATING DIGITAL SERVICES IN THE MOBILITY SECTOR

The spread of smartphones has created a myriad of new mobility services.[24] However, the sheer variety of services does not always translate into significant differences for customers. What many of the new services have in common is that they use an internet platform and a mobile app to connect users and vehicles and thus enable a far more efficient and flexible coordination than traditional taxi services. Invoking an emancipatory idea of mutually beneficial self-organization, such services are regularly labelled “ride sharing”. Yet, upon closer inspection, this quite often turns out to be illusory. Although some of these services are offered by private individuals driving their own vehicles, the service providers are controlled by powerful companies such as “Uber”, which manage the service via the digital platform and control it in economic terms.[25]

With these new forms of mobility, the question arises, how they can be successfully embedded in a future mobility concept and how legal regulation must be drafted in order to serve both economic and social rationales for regulation. As it turns out, the current regulatory framework is often insufficient to accommodate such services, as numerous litigations concerning “Uber” and other companies have demonstrated. Against this background, we will first look at the discussion in Germany and the recent amendment of the German Passenger Transportation Act [*Personenbeförderungsgesetz*] in particular (0.). After this, we will briefly deal with the role improved planning of urban mobility has to play in order to create a system of sustainable urban mobility (0.).

3.1. The German Passenger Transportation Act and new mobility services

[24] See e.g. *Krauss/Scherrer/Burghard/Schuler/Burger/Doll*, Sharing Economy in der Mobilität: Potenzielle Nutzung und Akzeptanz geteilter Mobilitätsdienste in urbanen Räumen in Deutschland, Working Paper No. WP P S 06/2020 of the Fraunhofer ISI, available at https://www.econstor.eu/handle/10419/215685 (accessed 18 Oct. 2021).

[25] Generally, such platforms are particularly characterised by network effects and concentration tendencies, as well as by the fact that the platform provider acts as gatekeeper and rule-setter. See the report by the *Kommission Wettbewerbsrecht 4.0* of the German Federal Ministry for Economic Affairs and Energy (Sept. 2019), p. 15 et seqq., available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=12 (accessed 18 Oct. 2021).

As in some other countries,[26] German courts have repeatedly rejected various "Uber" mobility services as incompatible with applicable law in the past years.[27] This points to some special features of the German Passenger Transportation Act (PTA).

3.1.1. *Fixed categories of transport services*

Most importantly, only such mobility services that fall into one of several *categories specified in the PTA* may be offered.[28] The types of services are on the one hand regular services that have fixed departure times and stops [*Linienverkehr*] and on the other hand occasional services [*Gelegenheitsverkehr*], which operate depending on individual demand. Within this framework, app-based mobility services may - at first glance - be classified as occasional services. However, many of them do not exactly fit into this predefined category. This is because they often take on multiple passengers with similar routes (so-called “ride pooling”). However, collecting different passengers with a similar destination is generally reserved for regular services.

Within the category of occasional services, there have - until recently - been two subcategories: taxi services and chauffeur services:

> 1.1.1) For the purpose of consumer protection, *taxi services* are particularly strictly regulated. For example, there is an obligation to carry (see § 47 (4) PTA). Therefore, a passenger may not be rejected simply because a route seems too short or because the pick-up point is too remote. Further, transport charges and conditions are not subject to individual negotiation but set by the authorities (§ 51 PTA). Also, the licensing authority may limit the number of taxi-licenses in order to protect the local taxi industry (§ 13 (4) PTA). Many, but by far not all, German cities make use of this opportunity.
>
> Many new mobility services such as “Uber” operate outside the local taxi con-

[26] See *Solmecke/Lengersdorf*, Rechtliche Probleme bei Sharing Economy, MMR 2015, p. 496; on Spain in particular see *Conde Gallego*, UBER in Spain, EuCML 2015, p. 62 et. seq.

[27] See e.g. Higher Administrative Court [*Oberverwaltungsgericht*] Berlin-Brandenburg, judgment from 10 April 2015, case 1 S 96.14; Higher Administrative Court [*Oberverwaltungsgericht*] Hamburg, judgment from 24 September 2014, case 3 Bs 175/14, ECLI:DE:OVGHH:2014:0924.3BS175.14.0A. Accordingly, they have also been said to violate competition law, see Federal Court of Justice [*Bundesgerichtshof*], judgment from 13 December 2018, case I ZR 3/16, ECLI:DE:BGH:2018:131218UIZR3.16.0; see prior Higher Regional Court [*Oberlandesgericht*] Frankfurt, judgment from 9 June 2016, case 6 U 73/15, ECLI:DE:OLGHE:2016:0609.6U73.15.0A; recently also Regional Court [*Landgericht*] Frankfurt, judgment from 19 December 2019, case 3-06 O 44/19, ECLI:DE:LGFFM:2019:1219.3.06O44.19.00.

[28] See further *Fehling/Schröter* (2020: 388 et seqq.).

tingents. Their attractiveness is not least due to them charging lower fares than traditional taxis. It is obvious that this can jeopardize the profitability and thus the functionality of traditional taxi services. The question, however, is whether, in view of new possibilities for urban mobility, the taxi industry in its traditional structures is still playing such a central role in guaranteeing urban mobility as it once did.

1.1.2) *Chauffeur services* are subject to other specific restrictions, which distinguish this type of traffic from taxi services. As to that, the so-called obligation to return (§ 49 (4) sentence 3 PTA) is especially important: If there is no immediate follow-up order, chauffeur services must first return to the company headquarters before being able to take on a new tour. In contrast, taxis can wait at various taxi stands and may be hailed on the road. Also, orders must be placed via the chauffeur company (§ 49 (4) sentence 2 PTA). Placing orders directly with the driver via App or by hailing a car on the road is not allowed.[29] Finally, collecting additional passengers en route (so-called "ride pooling") is illegal for chauffeur services (see § 49 (1) sentence 2, (2) sentence 1 PTA).

1.1.3) Each taken individually, all these restrictions appear absurd. However, otherwise chauffeur services, which are not subject to an obligation to carry and, above all, to prescribed charges, would threaten to displace taxi services, which are more heavily regulated in this respect.[30] Therefore, within the system of the PTA, almost all of these restrictions fulfil a legitimate purpose. Each of the classical types of mobility service is assigned a place within a transport market harmoniously divided into several segments. Hence, every category and every sub-category has a specific role to play in satisfying certain public transport needs: On the one hand, regular services with buses and trains allow for the transport of larger numbers of passengers according to standardised timetables. On the other hand, taxi services provide more individualised transport, especially for the elderly, the sick and business travellers, and close gaps left by the regular services. Lastly, chauffeur ser-

[29] *Ludwigs*, Rechtsfragen der Sharing Economy am Beispiel der Modelle Uber und Airbnb, NVwZ 2017, p. 1648.

[30] In Germany, the Federal Constitutional Court [*Bundesverfassungsgericht*] has relied on the theory of „ruinous competition" (hereunto *Fritsch*, Marktversagen und Wirtschaftspolitik, 10th edn. 2018, pp. 312 et seqq.) in order to justify the strict regulation of the taxi market; see judgment from 8 June 1960, case 1 BvL 53/55; see also judgment from 14 November 1989, cases 1 BvL 14/85 and 1 BvR 1276/84; judgment from 11 February 1992, case 1 BvL 29/87. The viability both of the economic theory and of its regulatory implications has been subject of fierce debate, see - *Fehling/Schröter* (2020: 390 et seq.).

vices provide particularly exclusive individual transport, not limited to a single route. The restrictions, which each of the service types is subject to in order to fulfil its specific role, is matched by the possibility to generate revenue within the respective market segment.

Altogether, this is based on the still valid consideration that local transport is a public service [*Daseinsvorsorge*],[31] in European terms: a service of general economic interest pursuant to Article 14 TFEU. This implies the assumption that the free market on its own will not produce a comprehensive supply at affordable prices.

This regulatory regime of well-balanced role allocation is shaken to its core by the appearance of atypical mobility services which do not equally balance regulatory burdens and market opportunities. Furthermore, the regulatory objectives traditionally associated with public services are nowadays being supplemented by the increasingly urgent matters of environmental and climate protection. A future-oriented regulatory regime must therefore consider various modes of transport and how their interlock and partly substitute each other. This also includes both individual transport and other forms of shared mobility, such as bike-sharing or electric scooters. The particularly strict regulatory concept underlying the PTA was not sufficiently open to development. It was thus not suitable to channel ride-sharing services in such a way that they can develop their potential for sustainable urban mobility.

3.1.2. *Recent reform of the Passenger Transportation Act*

The *recent reform of the Passenger Transportation Act*[32] does solve some but not all of the problems outlined above.

1.2.1) Firstly, it has now been made explicitly clear that digital platforms brokering transport services are subject to the Passenger Transportation Act (§ 1 (3) PTA). This is a precondition for both applying the obligation to carry and regulating their terms and condi-

[31] *Knauff*, Personenbeförderung auf der Straße einschließlich ÖPNV (§ 28), in: Ehlers/Fehling/Pünder (eds.) Besonderes Verwaltungsrecht vol. 1 (4th edn. 2019), rec. 1. The concept of *Daseinsvorsorge*, central to German regulatory theory, was first developed by *Forsthoff*, Die Verwaltung als Leistungsträger (1938), pp. 6 et seqq. (specifically on public transport pp. 36 et seq.); *Forsthoff*, Lehrbuch des Verwaltungsrechts (10th edn. 1973), pp. 368 et seqq.; see further *Kersten*, Die Entwicklung des Konzepts der Daseinsvorsorge im Werk von Ernst Forsthoff, 44 Der Staat (2005), pp. 543 et seqq.

[32] Gesetz zur Modernisierung des Personenbeförderungsrechts from 16 April 2021, BGBl. 2021 Teil I Nr. 19, pp. 822-832. For a discussion of an earlier version of the reform proposals see *Fehling/Schröter (*2020).

tions. However, digital platforms only need to be licensed under this act (cf. § 2 (1b) PTA) when they can be considered a service provider themself. This the case, when they effectively control the service (§ 1 (1a) PTA) and the actual drivers are left with only a limited scope of action.

1.2.2) Secondly and most importantly, there are *new regulations for ride pooling services*. The basic rationale of distinguishing certain pre-defined types of mobility services has been maintained - as well as the existing distinction between regular services and occasional services. However, under the new PTA, ride pooling services can now be considered to belong to each of those categories. As to that, the PTA distinguishes two types of ride pooling services:

1.2.2.1) On the one hand, pooling services which operate on demand but within a network of fixed stops can be classified and regulated as a new type of demand-driven regular transport [*Linienbedarfsverkehr*] (§ 44 PTA) and shall serve as a supplement to traditional scheduled services. These supplemental ride pooling services are also subject to the obligation to carry and to terms and conditions prescribed for regular public transport.

1.2.2.2) On the other hand, other ridesharing and ride pooling services are now classified and licensed as a new sub-category of occasional services, called occasional pooling services [*gebündelter Bedarfsverkehr*] (§ 50 PTA). This type of mobility service, where supply and demand are spontaneously coordinated via app and digital platform, corresponds to the business models of currently predominant providers such as "Uber", "MOIA" etc. Other than regular services, taxi, or chauffeur services, they can now - in principle - be freely offered on the market[33] without being burdened with specific public service obligations.

However, there is concern that such a new sub-sector, once relieved from regulatory burdens, will economically displace other essential traffic services. Therefore, the competent authorities are being given a set of regulatory tools to prevent them from cannibalising other public transport services (economically one speaks of “cream skimming”) and thus threatening the economic viability of the local public transport system as a whole. For example, when being licensed, such pooling services may be limited to a specific area or certain operating hours (§ 50 (2) sentence 2 PTA). Also, the licensing authority must - at least in urban areas - set a minimum “pooling-quota” [*Bündelungsquote*] which must be fulfilled (§ 50 (3) PTA). It means that for a certain amount of rides, passengers

[33] In German terminology: “*eigenwirtschaftlich*”.

must actually share a ride.[34] This is meant to prevent pooling services to compete with traditional taxi services. Besides, it also aims a realising the environmental potential of pooling services in urban mobility. If it is required to protect public transport interests, the competent authority may also dictate an obligation to return (like it exists for chauffeur services), an additional pooling-quota for rural areas or instructions as to where the vehicles may be parked (§ 50 (1) sentence 3, (4) PTA). To further mitigate competitive disadvantages for taxi services, whose terms and conditions are strictly regulated, and to maintain price advantages for regular services like buses and trains, the competent authority may further dictate minimum rates for pooling services (§ 51a (2-4) PTA).

1.2.3) In view of past experiences with low-paid drivers at "Uber" and similar companies, the Passenger Transportation Act now states that for occasional pooling services, the licensing authority may also dictate certain *social standards for the protection of employees*, regarding for example working hours, remuneration or work breaks (§ 50 (4) sentence 3 PTA). So far, EU-Regulation 1370/2007 (Art. 4 (5, 6)) only allows for this in connection with public service obligations in public service contracts; however, it does not prevent further-reaching national regulations.[35]

1.2.4) The *environmental dimension of public transport,* in particular the necessity to fight climate change, is now also expressed in various provisions of the Passenger Transportation Act. In general, § 1a PTA requires that the objectives of climate protection and sustainability are to be observed when implementing the Act. More specifically, provisions like the minimum pooling-quota also aim to reduce the volume of traffic for ecological reasons. Yet, we will not go into more detail here because this is not our main topic.

3.2. Prescient planning in order to create a system of sustainable urban mobility

Despite the latest changes to the Passenger Transportation Act, further reforms are needed to ensure that the state in the future meets its responsibility to guarantee sustainable urban mobility. As to that, we will single out one issue in particular:

A future system of urban mobility which is both demand-oriented and environmentally friendly will require diligent planning. This is particularly true when it comes to public services, which often rely on subsidies. Prescient planning allows the city to get an idea of

[34] More specifically, the pooling-quota is calculated as the ratio of the combined distance travelled by all passengers to the distance travelled by the vehicle within a certain period of time, § 50 (3) sentence 2 PTA.

[35] *Linke/Prieß*, commentary on Art. 4, in: Linke (ed.), VO (EG) 1370/2007 (2nd edn. 2019), rec. 71.

which mobility needs will have to be fulfilled in the future, which mobility services will be provided for commercially and on acceptable terms and which ones will have to be bought from transport companies by means of public service contracts. As mentioned above, this might also be ride pooling services if they are intended to supplement or even replace regular services but in their own right would not be economically viable. Yet, the need for prescient planning goes beyond merely satisfying public transport needs. Planning urban mobility is also necessary in order to permanently reduce individual traffic, not only to tackle congestion problems but mainly for reasons of environmental and climate protection.

For these reasons, almost all German states have local transport laws in which the (municipal) authorities are obliged to draw up local transport plans [*Nahverkehrspläne*].[36] However, these laws and the local transport plans focus almost exclusively on public transport with buses, trams and underground trains. The Passenger Transportation Act already requires calls for local transport plans to "integrate transport services across different means of transport" (§ 8 (3) sentence 2 PTA). Accordingly, local transport plans increasingly focus on mobility chains, for example in the form of "Park & Ride" and "Bike & Ride".[37] However, in the long run, the perspective must be broadened in order to include all relevant forms of transport and to coordinate them in an overall transport concept. Such is essential for fulfilling the constitutional guarantee of basic mobility in a cost-efficient way. The local transport laws should therefore be amended in such a way as to also include ride sharing and ride pooling services and their complementary function for local public transport.

IV. SOME GENERAL CONCLUSIONS

4.1. Challenges and regulatory approaches

By far not all insights derived from the mobility sector can be generalized. For example, finding drivers in a precarious situation as quasi-self-employed worker might be a phenomenon which is not specific to but particularly prevalent in the mobility sector.

[36] See e.g. § 10 of the law on local public transport for the state of North Rhine-Westphalia [*ÖPNVG NRW*].

[37] See e.g. the local transport plan of the City of Düsseldorf (2017), pp. 71 et seq., 101 et seqq., 170 es seq., available at https://www.duesseldorf.de/fileadmin/Amt66/verkehrsmanagement/pdf/NVP_Endfassung_2017.pdf (accessed 18 Oct. 2021).

However, with a view to consumer protection and social issues, some of the challenges and regulatory approaches can also be found in other sectors of the digital economy.

1.1) As is the case in much of (administrative) regulatory law, requiring *prior authorisation* of platform-based services can help to address problematic issues - including social ones - proactively and allow for a more effective enforcement of existing regulations.[38] As we have seen, the German Passenger Transportation Act now requires such prior authorisation of digital platforms brokering transport services if they can be considered a service provider themself.[39]

1.2) As far as platform driven services are *public services* or services of general economic interest (Art. 14 TFEU), a stricter regulatory framework might be needed. Amongst others, this may concern the terms and conditions of the services provided. Yet, looking at the mobility sector shows that such a need for regulation may well be limited to specific services. Different services offered via the same platform may hence require a different intensity of regulation, depending on how essential the provided services are an whether there are substitute services available. With a view to media platforms such as Facebook and their essential role in the democratic process, regulation might also include the need to guarantee a certain plurality of content.

1.3) Closely related to this is another important aspect in the digital platform economy: that of *equal and affordable access* to the services provided. This is particularly true if they can be considered public services for which the state has a responsibility to guarantee that they are universally available. As to that, it will depend on the circumstances, whether general anti-discrimination law will suffice or whether more specific regulation is required. Such might concern the pricing of services or an obligation to contract - both can be found in the Passenger Transportation Act.[40]

1.4) The growing *market power* of digital platforms - as well as them being characterised by network effects and concentration tendencies[41] - makes their users appear in particular need of protection. On the one hand, this is a matter of *consumer protection*. Below, we will discuss this in more detail with a view to the reputation systems of online platforms. On the other hand, it must be ensured that platform-based services do not displace existing public services without adequately replacing them. With a view to mobil-

[38] Cf. *Huber*, Überwachung (§ 45), in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (eds.), Grundlagen des Verwaltungsrechts, (2nd edn. 2013), rec. 102, 119 et seqq.

[39] See above 0.2.1.

[40] See above 0.1.

[41] See above n. 25.

ity services, it has been discussed, whether the constitutional guarantee of mobility might be at risk - at least for certain people like for example the elderly - when traditional taxi services are being replaced by novel mobility services.

4.2. Consumer protection and the reputation systems of online platforms

Reputation systems with numerical ratings and qualitative reviews are central to the functioning of the platform economy. Such systems are a major means to build trust between the parties involved and shall serve as equivalent safeguards to traditional consumer protection law. If a service provider or a customer has a five-star-rating, the other part can seemingly be assured that they will properly fulfil their contractual duties. Hence, reputation systems are among the most commonly cited examples for the advantages of self-regulation.

2.1) Up to now, the reputation system is within the platform´s responsibility alone. The management of the system and the underlying algorithm thus basically remain a black box.[42] For example, it is not clear whether and under which circumstances platforms delete certain reviews because they are judged to be impertinent or offending. Also, we do not know whether due to statistical or other reasons the platform eliminates some of the user-generated ratings when calculating the average rating or when compiling a statistic summary.

Several articles in the field of behavioural economics and psychology cast some doubt on the validity of such rating systems.[43] Many existing review platforms have been shown to generate implausible distributions of ratings. The literature has linked the abundance of positive reviews on online platforms - not only, but including such of the sharing economy[44] - to at least four underlying phenomena: herding behaviour, whereby prior ratings subtly bias the evaluation of subsequent reviewers; under-reporting of negative experiences because reviewers fear retaliatory reviews on platforms that allow and encourage mutual reviewing; self-selection where consumers who a priori are more attracted to a service are also more likely to use and review it, and, most problematic, strategic manipu-

[42] Cf. *Pasquale*, The Black Box Society: The Secret Algorithms That Control Money and Information (2015).

[43] See *Busch/Schulte-Nölke/Wiewiórowska-Domagalska/Zoll* (2016: 9) with further references.

[44] For example, according to a study in 2015 (2018) 94% (91 %) of all properties getting a star rating of 4.5 or even the maximum of 5 stars, *Zervas/Proserpio/Byers*, A First Look at Online Reputation on Airbnb: Where Every Stay is Above Average (2020), pp. 3, 7, available at https://ssrn.com/abstract=2554500 (accessed 19 Oct. 2021).

lation of reviews by firms who seek to artificially brush up their online image.[45] Additionally, social bots offer opportunities to manipulate a competitor's average ratings on a large scale.[46] At the very least, when ratings are optional, they may be unrepresentative.[47]

It is questionable whether the economic self-interest of the platform provider will lead to sufficient measures to improve the reputational system. On the one hand, providers of digital platforms will typically be interested in identifying and delisting or blocking service providers (and customers) with a bad performance or illegal conduct because such "black sheep" damage the reputation of the platform itself. On the other hand, platforms might be even more interested in an overall high rating of their service providers because this arguably encourages customers to prefer their platform over competitors.

2.2) Therefore, we should not exclusively rely on self-regulation to guarantee functioning reputation systems that safeguard both consumer and public interests. As to that, one can think of at least four different means for regulating a platform´s rating and review system.

Firstly, sharing platforms could be ordered to provide detailed information about their rating mechanisms to public authorities. Gathering this knowledge is a precondition for future legislative or administrative action. Admittedly, disclosing the internal operations of such software affects elemental business secrets of the sharing company.[48] Precautionary measures must thus be taken to guarantee that the information is only revealed to the competent authority; if it comes to legal proceedings involving competitors, the administrative agency or court must proceed "in camera".[49] For the same reason, only certain

[45] *Zervas/Proserpio/Byers* (2020: 2) with further references; also see *Edelman/Geradin* (2016: 316) with further references; *Hu/Pavlou/Zhang*, On Self-Selection Biases in Online Product Reviews, 41 MIS Quarterly (2017), p. 453 also takes into account „paid reviewers", in order to „promote or damage a product", however considering the effect to be minor.

[46] *Dankert*, Verfälschung von Datenbeständen durch Social Bots, in: Hoffmann-Riem (ed.), Big Data - Regulative Herausforderungen (2018), pp. 157 et seqq.; *Libertus*, Rechtliche Aspekte des Einsatzes von Social Bots de lege lata und de lege ferenda, ZUM 2018, p. 20; also see the empirical research conducted by *Ross/Pilz/Cabrera/Brachten/Neubaum/Stieglitz*, Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks, 28 European Journal of Information Systems (2019), pp. 394 et seqq.

[47] *Edelman/Geradin* (2016: 316) with further references; also see *Hu/Pavlou/Zhang* (2017: 453, 466).

[48] In a different context *Fehling*, Freier Informationszugang zwischen öffentlichen und privaten Interessen, DVBl. 2017, pp. 79 et seqq.

[49] *Knauff*, Regulierungsverwaltungsrechtlicher Rechtsschutz, 98 VerwArch (2007), pp. 405 et seqq.; *von Danwitz*, Der Schutz von Betriebs- und Geschäftsgeheimnissen im Recht der Regulierungsverwaltung, DVBl. 2005, pp. 597 et seqq.

information can be given to the public. Such a transparency requirement - although very general and vague - regarding the functioning of algorithms used by media intermediaries can be found in § 93 of the new German interstate treaty on media law [*Medienstaatsvertrag*],).[50] To some extent, this might serve as an example for disclosure requirements concerning basic features of platform algorithms in other sectors. Even if such basic transparency might have a limited effect on the general public, it might lead to some scrutiny by specialised public interest organisations - like the German *Chaos Computer Club*. However, an algorithm remains a black box when the algorithm itself develops by way of self-learning processes.[51]

Secondly, one could set certain minimal standards that a reputation system has to meet. This could include the duty to properly inform the service providers, the customers, and the public about the mode of operation of the reputation system. It would be up to the platform to shape this information in such a way that it is meaningful and as accurate as possible. This should enable consumers and contractors to better judge the validity of the rating system and could help to correct for inherent biases.

Thirdly, the platform must face the duty to delete or even correct wrong data within its reputation system on a notice and take down-basis.[52] As far as personal data is affected (which is certainly true for qualitative reviews), this is already the law under the General Data Protection Regulation (GDPR).[53] For facilitating judicial review, the platform should be mandated to disclose the internal decision-procedure when dealing with a request to delete or correct such data within its reputation system.[54] Insofar, the current draft for a Digital Services Act[55] lays down some basic obligations (Chapter III Section 2), applicable to providers of hosting services, supplemented by obligations for all online platforms

---

[50] For some details see *Flamme*, Schutz der Meinungsvielfalt im digitalen Raum, MMR 2021, p. 772.

[51] See *Hoffmann-Riem*, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (ed.) Big Data - Regulative Herausforderungen (2018), pp. 47 et seqq.; *Wischmeyer*, Regulierung intelligenter Systeme, 143 AöR (2018), pp. 43 et seq.

[52] See *Cauffman*, The Commission's European Agenda for the collaborative Economy - (Too) Platform and Service Provider Friendly?, EuCML 2016, p. 239.

[53] See Art. 16, 17 GDPR. Even though, the explicit wording (only) states a „right to erasure", the prevailing opinion generally assumes a corresponding obligation to erase said data without a request, see *Paal*, in: Paal/Pauly (eds.), DSGVO (3rd edn. 2021), Art. 17 rec. 20 with further references.

[54] Cf., *Fehling/Leymann*, Der neue Strukturwandel der Öffentlichkeit: Wie lassen sich die sozialen Medien regulieren?, AfP 2019, p. 113; more generally *Eifert*, Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen, NJW 2017, pp. 1450 et seqq.

[55] COM/2020/825 (final).

(Chapter III Section 3), excluding those that qualify as micro or small enterprises. However, there are no provisions addressing reputation systems in particular. So far, the focus is very much on the removal of illegal content (including such violating consumer protection laws) and content violating the platform's terms and conditions. Additional reporting obligations to manage systemic risks (Chapter III Section 4) do only apply to very large online platforms like Google or Facebook and will (for now) probably not be relevant for digital mobility platforms.

Fourthly, the platform provider could also be forced to monitor the functioning of its reputation system with a view to detecting manipulation by third parties. However, such an obligation would only be compatible with the e-Commerce Directive[56] as far as the platform is not limited to a passive role of hosting reviews posted by third parties. Yet, the ECJ has ruled that the hosting exemptions in Art. 14, 15 of the e-Commerce Directive only apply when "the (platform) provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored".[57] This, however, must be judged not in general but with regard to the specific setting in question. Also, a platform's service can only be in part covered by the privileges of the directive. Since there is some reason to believe that many platform providers are so closely linked to the provision of the real-world services that they might be considered to not be limited to a mere passive role of storing data,[58] it would only be a matter of proportionality in how far national law could delegate monitoring-obligations to the platform provider. This will probably not change under the Digital Services Act, because Art. 3-9 of the draft DSA are modelled after the e-Commerce-Directive.[59]

4.3. Final remarks

The advantages of digital platforms and a platform-economy promise both new and better services. Such is also the case for (urban) mobility. However, the free market alone will not always do the job. Instead, we must look for an adequate regulatory framework.

[56] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[57] ECJ, Judgment of the Court (Grand Chamber) from 23 March 2010, Joined Cases C-236/08 to C-238/08 (Google France/Louis Vuitton), ECLI:EU:C:2010:159; confirmed in Judgment of the Court (Grand Chamber) from 12 July 2011, Case C-324/09 (L'Oréal SA et. al/eBay), ECLI:EU:C:2011:474. Both judgments are discussed by *Cauffman* (2016: 238-239).

[58] Cf. *Terryn* (2016: 51).

[59] See Recital (16) of the draft DSA, COM/2020/825 (final).

This includes an intelligent mixture of both (regulated) self-regulation and direct regulation by the state to compensate potential market failures. Important regulatory goals are protecting consumer interests and guaranteeing the provision of public services that are of general interest. Both can be closely interlinked with other traditional economic rationales for regulation. This also holds true for the mobility sector.

The main focus of any regulation is still the dominant market power of such platforms. However, this is not only an issue of competition law. The EU-Commission's current proposals for a Digital Services Act and a Digital Markets Act are a first step towards a general regulatory framework for platform-based services. A more ambitious approach could and should also include some basic rules for reputational systems of such platforms, setting in place a system of regulated self-regulation for the sake of consumer protection.

However, we also need sector-specific regulation. Such is needed when regulating for social rationales that go beyond traditional employment law. This includes guaranteeing accessible and affordable services of general (economic) interest. Although this concerns several sectors of the digital economy, every sector has its specific features and necessities. With a view to our topic, there is the special need to guarantee basic mobility for all people. To reach this goal in a the efficient and environmentally friendly way, new ride pooling services that are offered via digital platforms can supplement traditional public transport. This, however, requires that some (but not all) of such platform-based services are subject to specific obligations like an obligation to transport and certain tariff-regulations. Furthermore, social as well as environmental goals can only be reached with prescient planning and focussing on mobility chains.

Social goals and consumer protection are closely interlinked not only in the digital economy. However, they are not identical. Consumer protection does not only focus on those that are economically or socially disadvantaged but addresses structural imbalances mainly because of information asymmetries. Nonetheless, consumer protection addresses the "weaker" side of the contractual relationship and therefore has a strong social impact, even if it is based upon the model of an "average and well informed consumer".[60]

The mobility sector (in Germany mainly the Passenger Transport Act) also shows that technological and economic changes call for one reform after the other. It seems as if we are far from having reached the end of developing towards a platform economy. There-

[60] See, e.g., Recital (23) of the draft DSA, COM/2020/825 (final). Regarding the change in the underlying consumer-role model see *Pfeiffer*, in: Grabitz/Hilf/Nettesheim (eds.), Das Recht der Europäischen Union (73. edn. 2021), rec. 21 et seqq. with further references.

fore, we are also far from having reached the end of debates about the need for legal regulation to cope with these economic developments.

V. BIBLIOGRAPHY

BALDWIN, Robert / CAVE, Martin / LODGE, Martin (2012): 'Understanding Regulation: Theory, Stretegy, and Practice', 2nd edn. Oxford University Press 2012.

BERG, Wilfried / FISCH, Stefan / SCHMITT GLAESER, Walter / SCHOCH, Friedrich / SCHULZE-FIELITZ, Helmuth (eds.), 'Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates', Die Verwaltung, Beiheft 4, Duncker & Humblot 2001.

BUSCH, Christoph / SCHULTE-NÖLKE, Hans / WIEWIÓROWSKA-DOMAGALSKA, Aneta / ZOLL, Fryderyk (2016): 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law? ', Journal of European Consumer and Market Law (EuCML) 2016, pp. 3-10.

CAUFFMANN, Caroline (2016): 'The Commission's European Agenda for the collaborative Economy - (Too) Platform and Service Provider Friendly?', Journal of European Consumer and Market Law (EuCML) 2016, pp. 235-243.

COGLIANESE, Cary / MENDELSON, Evan (2012): 'Meta-Regulation and Self-Regulation', in: BALDWIN, Robert / CAVE, Martin / LODGE, Martin (eds.), The Oxford Handbook of Regulation, Oxford University Press 2012, pp. 146-168.

CONDE GALLEGO, Beatriz (2015), 'UBER in Spain', Journal of European Consumer and Market Law (EuCML) 2015, pp. 62-63.

DANKERT, Kevin (2018): 'Verfälschung von Datenbeständen durch Social Bots', in: HOFFMANN-RIEM, Wolfgang (ed.), 'Big Data - Regulative Herausforderungen', Nomos, pp. 157-166.

VON DANWITZ, Thomas (2005): 'Der Schutz von Betriebs- und Geschäftsgeheimnissen im Recht der Regulierungsverwaltung', Deutsches Verwaltungsblatt (DVBl.) 2005, pp. 597-605.

DAVIES, Rob (2017): 'Uber loses appeal in UK employment rights case', The Guardian (10 November 2017), available at https://www.theguardian.com/technology/2017/nov/10/uber-loses-appeal-employment-rights-workers (accessed 18. Oct. 2021).

EDELMANN, Benjamin G. / GERADIN, Damien (2016): 'Efficiencies and Regulatory Shortcuts: How should we regulate Companies like Airbnb and Uber?', Stanford Technology Law Review vol. 19, pp. 293-328.

EIFERT, Martin (2012), 'Regulierungsstrategien', in: HOFFMANN-RIEM, Wolfgang / SCHMIDT-AßMANN, Eberhard / VOßKUHLE, Andreas (eds.), 'Grundlagen des Verwaltungsrechts' (vol. I), 2nd edn. C.H. Beck 2012, § 19.

EIFERT, Martin (2017): 'Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen', Neue Juristische Wochenschrift (NJW) 2017, pp. 1450-1454.

FEHLING, Michael (2017): 'Freier Informationszugang zwischen öffentlichen und privaten Interessen', Deutsches Verwaltungsblatt (DVBl.) 2017, pp. 79-88.

FEHLING, Michael (2020): 'Urbane Verkehrskonzepte der Zukunft - Ökonomische versus ordnungsrechtliche Instrumente', Zeitschrift für Umweltrecht (ZUR) 2020, pp. 387-393.

FEHLING, Michael / LEYMANN, Matthias (2020): 'Der neue Strukturwandel der Öffentlichkeit: Wie lassen sich die sozialen Medien regulieren?', Archiv für Presserecht (AfP) 2020, pp. 110-119.

FEHLING, Michael / SCHRÖTER, Nico (2020): 'Regulierungsansätze für plattformgestützte Mobilitätsdienste - Reformbedarf und Reformbestrebungen', Die Verwaltung vol. 53, pp. 381-420.

FINCK, Michèle (2018): 'Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy', European Law Review (E.L. Rev.) 2018, vol. 43 no. 1, pp. 47-68.

FLAMME, Florian (2021): 'Schutz der Meinungsvielfalt im digitalen Raum', Multimedia und Recht (MMR) 2021, pp. 770-774.

FORSTHOFF, Ernst (1938): 'Die Verwaltung als Leistungsträger', Kohlhammer.

FORSTHOFF, Ernst (1973): 'Lehrbuch des Verwaltungsrechts', 10th edn., C.H. Beck.

FRITSCH, Michael (2018): 'Marktversagen und Wirtschaftspolitik', 10th edn. Vahlen 2018.

GIELEN, Nico / UPHUES, Steffen (2021): 'Digital Markets Act und Digital Services Act: Regulierung von Markt- und Meinungsmacht durch die Europäische Union', Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2021, pp. 627-637.

GRIFFITH, Keyawna (2019): 'The Uber Loophole that protects surge pricing', Virginia Journal of Social Policy & the Law vol. 26 no. 1, pp. 34-64.

HEINRICHS, Harald / GRUNENBERG, Heiko (2012): 'Sharing Economy: Auf dem Weg in eine neue Konsumkultur?', available at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-427486 (accessed 18 Oct. 2021).

HOFFMANN-RIEM, Wolfgang (2016), 'Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext, in: FEHLING, Michael / SCHLIESKY, Utz (eds.), 'Neue Macht- und Verantwortungsstrukturen in der digitalen Welt', Nomos 2016.

HOFFMANN-RIEM, Wolfgang (2018): 'Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data', in: HOFFMANN-RIEM, Wolfgang (ed.), 'Big Data - Regulative Herausforderungen', Nomos, pp. 9-78.

HU, Nan / PAVLOU, Paul A. /ZHANG, Jie (2017): 'On Self-Selection Biases in Online Product Reviews', Management Information Systems Quarterly (MIS Quarterly) vl. 41 no. 2, pp. 449-471.

HUBER, Peter M. (2013): 'Überwachung', in: HOFFMANN-RIEM, Wolfgang / SCHMIDT-AßMANN, Eberhard / VOßKUHLE, Andreas (eds.), 'Grundlagen des Verwaltungsrechts' (vol. III), 2nd edn. C.H. Beck 2013, § 45.

KATZ, Vanessa (2015): 'Regulating the Sharing Economy', 30 Berkeley Technology Law Journal, pp. 1067-1126.

KERSTEN, Jens (2005): 'Die Entwicklung des Konzepts der Daseinsvorsorge im Werk von Ernst Forsthoff', Der Staat vol. 44, pp. 543-569.

KNAUFF, Matthias (2007): 'Regulierungsverwaltungsrechtlicher Rechtsschutz', Verwaltungsarchiv (VerwArch) vol. 98, pp. 382-409.

KNAUFF, Matthias (2019), Personenbeförderung auf der Straße einschließlich ÖPNV (§ 28), in: EHLERS, Dirk / FEHLING, Michael / PÜNDER, Hermann (eds.) Besonderes Verwaltungsrecht vol. 1, 4th edn. C.F. Müller 2019, pp. 1204-1233.

KNIEPS, Günther (2018): 'Network Economics of Shared Mobilty', Network Industries Quarterly vol. 20 no. 3, pp. 9-12.

KOMMISSION WETTBEWERBSRECHT 4.0 (2019): 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft', available at https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=12 (accessed 18 Oct. 2021).

KRAUSE, Rüdiger (2017): 'Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0', NZA-Beilage 2017, pp. 53-59.

KRAUSS, Konstantin / SCHERRER, Aline / BURGHARD, Uta / SCHULER, Johannes / BURGER, Axel Michael / DOLL, Claus (2020): 'Sharing Economy in der Mobilität: Potenzielle Nutzung und Akzeptanz geteilter Mobilitätsdienste in urbanen Räumen in Deutschland', Working Paper No. WP P S 06/2020 of the Fraunhofer ISI, available at https://www.econstor.eu/handle/10419/215685 (accessed 18 Oct. 2021).

LEE, Je Seung (2019), 'French court follows UK in ruling against Uber in 'employment' contract case', The Telegraph (11 Jan. 2019), available at https://www.telegraph.co.uk/news/2019/01/11/french-court-follows-uk-ruling-against-uber-employment-contract/ (accessed 18. Oct. 2021).

LIBERTUS, Michael (2018): 'Rechtliche Aspekte des Einsatzes von Social Bots de lege lata und de lege ferenda', Zeitschrift für Urheber- und Medienrecht (ZUM) 2018, pp. 20-26.

LINKE, Benjamin / PRIEß, Hans-Joachim (2019), commentary on Art. 4, in: LINKE, Benjamin (ed.), VO (EG) 1370/2007 über öffentliche Personenverkehrsdienste, Kommentar, 2nd edn. C.H. Beck 2019.

LUDWIGS, Markus (2017): 'Rechtsfragen der Sharing Economy am Beispiel der Modelle Uber und Airbnb', Neue Zeitschrift für Verwaltungsrehct (NVwZ) 2017 pp. 1646-1653.

DI MATTEO, Larry A. (2016): 'Regulation of Share Economy: A Consistently Changing Environment', in: SCHULZE, Reiner / STAUDENMAYER, Dirk (eds.), 'Digital Revolution: Challenges for Contract Law in Practice', Nomos/Hart 2016, pp. 89-112.

MONOPOLIES COMMISSION (2016): 'Twenty-first Biennial Report of the German Monopolies Commission (Monopolkommission) in accordance with Sec. 44 (1) sentence 1 of the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen - GWB) ', English excerpt available at https://www.monopolkommission.de/images/HG21/HGXXI_Chapter_V.pdf (accessed 18. Oct. 2021).

PAAL, Boris P. (2021): commentary on Art. 17, in: PAAL, Boris P. / PAULY, Daniel A. (eds.), Datenschutz-Grundverordnung, 3rd edn. C.H. Beck 2021.

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

PFEIFFER, Thomas (2021): commentary on Art. 169, in: GRABITZ, Eberhard / HILF, Meinhard / NETTESHEIM, Martin (eds.), Das Recht der Europäischen Union, 73. edn. C.H. Beck 2021.

RODI, Michael (2014): 'Ökonomische Analyse des Öffentlichen Rechts', Springer Gabler 2014.

ROSS, Björn / PILZ, Laura / CABRERA, Benjamin / BRACHTEN, Florian / NEUBAUM, German / STIEGLIETZ, Stefan (2019): 'Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks', European Journal of Information Systems, vol. 28 no. 4, pp. 394-412.

SOLMECKE, Christian / LENGERSDORF, Bonny (2015): 'Rechtliche Probleme bei Sharing Economy: Herausforderungen an die Gesetzgebung auf dem Weg in eine geteilte Welt', Multimedia und Recht (MMR) 2015, pp. 493-497.

TERRYN, Evelyne (2016): 'The Sharing Economy in Belgium - A Case for Regulation', Journal of European Consumer and Market Law (EuCML) 2016, pp. 45-51.

WISCHMEYER, Thomas (2018): 'Regulierung intelligenter Systeme', Archiv des öffentlichen Rechts (AöR) vol. 143, pp. 1-66.

ZERVAS, Georgios / PROSERPIO, Davide / BYERS, John (2020): 'A First Look at Online Reputation on Airbnb: Where Every Stay is Above Average' (December 2020), available at: https://ssrn.com/abstract=2554500 (accessed 19 Oct. 2021).

LA PROPUESTA DE REGLAMENTO DE INTELIGENCIA ARTIFICIAL DE LA UE Y LOS SISTEMAS DE ALTO RIESGO [1]

Por

ALBA SORIANO ARNANZ
Profesora Ayudante Doctora de Derecho Administrativo
Universitat de València

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

ABSTRACT: The growing use of artificial intelligence in all kinds of contexts has generated the need for a specific legal framework that addresses the risks produced by automated systems. The new proposal of a European Artificial Intelligence Act tries to accomplish said task. This paper focuses on some of the provisions contained in said regulatory proposal, in particular, those which address high-risk artificial intelligence systems. In doing so, it aims to highlight some of the positive aspects of the future Regulation but also its limitations and shortcomings.

KEYWORDS: Artificial intelligence, automated decision-making, algorithms, risks.

RESUMEN: El creciente uso de la inteligencia artificial en toda clase de contextos ha generado la necesidad de establecer un marco jurídico específico que aborde los riesgos producidos por los sistemas automatizados. La nueva propuesta de Ley Europea de Inteligencia Artificial trata de cumplir dicha tarea. Este trabajo se centra en algunas de las disposiciones contenidas en dicha propuesta normativa, en particular, las que abordan los sistemas de inteligencia artificial de alto riesgo. Con ello, se pretende destacar algunos de los aspectos positivos del futuro Reglamento, pero también sus limitaciones y carencias.

PALABRAS CLAVE: Inteligencia artificial, decisiones automatizadas, algoritmos, riesgos.

SUMARIO: I. INTRODUCCIÓN. II. La necesidad de un marco jurídico para la inteligencia artificial. 1. El creciente uso de sistemas de inteligencia artificial. 2. Los riesgos del creciente uso de sistemas de inteligencia artificial. 3. Límites y deficiencias de las normas existentes. III. LA PROPUESTA DE REGLAMENTO DE INTELIGENCIA ARTIFICIAL (EN GENERAL). 1. Estructura. 2. Ámbito de aplicación. 2.1. Objetivo. 2.2. Subjetivo y territorial. 3. Un enfoque basado en el riesgo. IV. LA REGULACIÓN DE LOS SISTEMAS DE ALTO RIESGO. 1. La clasificación de los sistemas de alto riesgo. 1.1. El problema de los sistemas empleados por las grandes plataformas

[1] Este trabajo se ha desarrollado dentro de la SHINE Jean Monnet Network (Sharing Economy and Inequalities across Europe) donde varias Universidades europeas, coordinadas por la Universitat de València, están estudiando estas cuestiones con el apoyo de la Comisión Europea (611585-EPP-1-2019-1-ES-EPPJMO-NETWORK).

digitales. 2. Requisitos de los sistemas de alto riesgo y obligaciones de los operadores. 2.1. Requisitos. 2.1.1. Sistema de gestión de riesgos. 2.1.2. Datos y gobernanza de datos. 2.1.3. Requisitos relacionados con la transparencia, explicabilidad y comprensibilidad de los sistemas. 2.1.4. Intervención humana. 2.2. Obligaciones de los operadores. 3. Autoridades de control y evaluación de la conformidad. 4. Una base de datos para sistemas de alto riesgo independientes. V. Conclusiones finales. VI. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

El pasado 21 de abril de 2021 fue publicada la propuesta de Reglamento de Inteligencia Artificial de la Unión Europea, también conocida como "Ley de Inteligencia Artificial"[2]. Esta propuesta de texto normativo, a la que todavía le queda un largo camino por recorrer, trata de dar respuesta a los diferentes riesgos derivados del creciente uso de los sistemas de inteligencia artificial. La publicación de esta propuesta debe ser entendida en el marco y como parte del bloque normativo recientemente propuesto por la UE con el objetivo de hacer frente a los retos jurídicos que presenta una sociedad cada vez más dominada por el mundo digital. Además de la "Ley de Inteligencia Artificial" este bloque normativo incluye las propuestas de Reglamento de Servicios Digitales[3], de Mercados Digitales[4] y de Gobernanza de Datos[5].

El presente trabajo se centra en la regulación de aquellos sistemas de inteligencia artificial empleados para analizar el comportamiento humano y la realidad social, concretamente, en aquellos que son susceptibles de generar mayores riesgos para los derechos fundamentales de las personas. Para ello, en primer lugar, se establecen las razones por las que es necesario un marco jurídico específico que regule la inteligencia artificial. Entre estas razones cabe desatacar el creciente uso de sistemas de inteligencia artificial en toda clase de contextos y, sobre todo, aquellos ámbitos que afectan de manera más directa a los derechos de las personas; los riesgos que genera el creciente uso de herramientas de inteligencia artificial y las deficiencias de los marcos jurídicos existentes que pueden ser de aplicación a estos sistemas.

---

[2] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. Disponible el 11 de septiembre de 2021 en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN

[3] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE. Disponible el 11 de septiembre de 2021 en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=COM:2020:825:FIN

[4] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales). Disponible el 11 de septiembre de 2021 en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020PC0842

[5] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos). Disponible el 11 de septiembre de 2021 en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52020PC0767

A continuación, los apartados III y IV del presente trabajo analizan, de manera general, la regulación de los sistemas de inteligencia artificial de alto riesgo que realiza la propuesta de nuevo Reglamento de Inteligencia Artificial de la UE. Además de realizar un análisis expositivo del contenido de dicha propuesta normativa a nivel explicativo, también se lleva a cabo un análisis crítico de aquellos aspectos en los que se considera que la propuesta del Reglamento adolece de deficiencias que impedirán un control efectivo de los riesgos generados por los sistemas de Inteligencia Artificial. Asimismo, se mencionarán aquellos aspectos en los que la propuesta de Reglamento contribuye a llenar algunas de las lagunas del marco jurídico en materia de protección de datos. En cualquier caso, conviene resaltar que el análisis aquí realizado no pretende ser un estudio pormenorizado de toda la propuesta normativa sino ofrecer una visión general de algunos de sus aspectos.

II. LA NECESIDAD DE UN MARCO JURÍDICO PARA LA INTELIGENCIA ARTIFICIAL

1. El creciente uso de sistemas de inteligencia artificial

Durante los últimos años hemos asistido a un creciente uso de sistemas de inteligencia artificial empleados para analizar el comportamiento humano y la realidad social en toda clase de contextos. Estos sistemas resultan especialmente útiles a la hora de agilizar y aumentar la eficiencia de los procesos decisorios que tienen lugar en múltiples sectores y que, de manera directa o indirecta, afectan a seres humanos. Los recientes desarrollos en la capacidad de almacenamiento y procesamiento de datos de los sistemas informáticos han contribuido a facilitar la toma de decisiones tanto en el sector público como en el sector privado, en ámbitos como la sanidad, la educación, la gestión del empleo o la concesión de préstamos[6].

Asimismo, las usuarias y usuarios de toda clase de servicios digitales constantemente interactúan con sistemas de inteligencia artificial. Por ejemplo, las recomendaciones que realizan los motores de búsqueda son el resultado que ofrecen los algoritmos que los integran. Lo mismo sucede con las recomendaciones de páginas realizadas por redes sociales como *Instagram* o con el orden en el que aparecen las publicaciones en estas plataformas. También en el ámbito digital, gracias al uso de sistemas de inteligencia artificial, se crean perfiles de cada persona usuaria, en virtud de los cuales le es

[6] COGLIANESE, Cary y LEHR, David, (2017): "Regulating by robot: administrative decision making in the machine-learning era", *The Georgetown Law Journal*, vol. 105, nº 5, pág. 1162; O'NEIL, Cathy, (2017): *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin Books, Londres, pág. 70.

mostrada publicidad relativa a aquellos productos o servicios que, en principio, más le pueden interesar[7].

Así pues asistimos a un evidente cambio de paradigma en toda clase de toma de decisiones. Quizás el cambio es menor, o al menos resulta menos obvio, en el ámbito estrictamente digital, esto es, en la interacción directa con plataformas y aplicaciones digitales. Esto es así por cuanto que el funcionamiento de esta clase de servicios implica claramente el uso de tecnologías de procesamiento automatizado de datos. Sin embargo, no debemos menospreciar el grado de evolución en la capacidad de los sistemas de inteligencia artificial empleados por herramientas como Google, Facebook o plataformas como Amazon a la hora de acceder y procesar información relativa a personas físicas y jurídicas y, por ejemplo, crear perfiles enormemente precisos de cada una de las personas usuarias, adaptando así los resultados ofrecidos a cada una de ellas. Esta realidad conlleva también importantes riesgos que se abordarán más adelante y a los que también se debe hacer frente desde el ordenamiento jurídico.

Sin embargo, el significativo cambio que supone el creciente uso de sistemas de inteligencia artificial es sobre todo llamativo en aquellos ámbitos y procesos decisorios en los que tradicionalmente intervenían únicamente seres humanos. También podemos destacar aquellos contextos en los que, si bien se vienen empleando sistemas informáticos desde hace años, su uso no ha sido demasiado evidente o su capacidad de almacenamiento, procesamiento o autoaprendizaje era mucho menor. Este es el caso de muchas entidades bancarias que ya empleaban sistemas informáticos para analizar el perfil financiero de cada una de sus clientas y clientes.

2. Los riesgos del creciente uso de sistemas de inteligencia artificial

Teniendo en cuenta los numerosos trabajos existentes en relación con los riesgos generados por el uso de sistemas de inteligencia artificial, el presente estudio no se detiene en detallarlos. Sin embargo, sí consideramos conveniente, al menos, señalar cuáles son esos riesgos que justifican el desarrollo de un nuevo marco jurídico en materia de inteligencia artificial.

En este sentido, estos sistemas se caracterizan por una enorme opacidad, tanto en lo que a su uso se refiere[8] como, en no pocas ocasiones, en cuanto a su contenido que, bien por estar protegido por intereses contrapuestos (derechos de propiedad intelectual),

[7] BOIX PALOP, Andrés, (2021): "Digital platforms competition regulatory challenges", *Revista General de Derecho de los Sectores Regulados*, nº 8.

[8] BAROCAS, Solon y SELBST, Andrew (2018): "The intuitive appeal of explainable machines", *Fordham Law Review*, vol. 87, nº 3, págs. 1091-1092.

bien por su enorme complejidad[9], no permite un grado de transparencia suficiente como para comprender las decisiones adoptadas por el sistema. La opacidad de estos sistemas es especialmente problemática en el ámbito de las Administraciones públicas por la especial intensidad con la que se deben aplicar los requisitos de transparencia a los procesos decisorios adoptados por estas[10].

Además, la falta de transparencia dificulta el ejercicio efectivo de los derechos propios de un debido proceso. Resulta complicado para una persona afectada por una decisión basada en un tratamiento automatizado de datos defender su posición cuando ni siquiera conoce las razones por las que el sistema ha tomado la decisión. Es más, en general, no se han establecido mecanismos y procedimientos que garanticen la defensa de los derechos e intereses de las personas afectadas por herramientas o sistemas de inteligencia artificial[11].

También se ha llamado la atención sobre los sesgos y errores que pueden cometer los sistemas automatizados de procesamiento de datos. Uno de los problemas de tratar de analizar y medir el comportamiento humano y la realidad social es que dicho análisis nunca puede ser plenamente objetivo. La sociedad es el producto de construcciones humanas elaboradas desde diferentes perspectivas.

Asimismo, los sistemas de inteligencia artificial de los que se ocupa este trabajo también han demostrado tener un potencial significativo en la perpetuación de las estructuras históricas de discriminación que han situado, y todavía hoy sitúan, a las personas pertenecientes a determinados grupos en una posición de desventaja. En los últimos años han salido a la luz múltiples supuestos de sistemas algorítmicos que discriminan (o son empleados por seres humanos para discriminar) a las personas pertenecientes a grupos desaventajados. Asimismo, no son pocos los casos en los que, sin tratarse de supuestos de discriminación algorítmica, el uso de estos sistemas ha contribuido a perpetuar la desigualdad, por ejemplo, a través de la exposición de estereotipos negativos en motores de búsqueda[12].

---

[9] BURRELL, Jenna (2016): "How the machine 'thinks': understanding opacity in machine learning algorithms", *Big Data & Society*, vol. 3, nº 1, pág. 5.

[10] CERRILLO I MARTÍNEZ, Agustí, (2019): "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo*, nº 50, pág. 18; MESTRE DELGADO, Juan Francisco, (2018): "Una reflexión sobre la regulación constitucional del Derecho administrativo", *Corts: Anuario de Derecho Parlamentario*, nº extra 31, pág. 384.

[11] KAMINSKI, Margot, (2019): "Binary governance: Lessons from the GDPR's approach to algorithmic accountability", *Southern California Law Review*, vol. 92, núm. 6, 2019, págs. 1538-1539.

[12] O'NEIL, Cathy (2017); NOBLE, Safiya, (2018): *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York University Press, Nueva York, p. 80.

Finalmente, los sistemas de inteligencia artificial también pueden emplearse con el objetivo de manipular a las personas que interactúan con ellos[13].

3. Límites y deficiencias de las normas existentes

Como es lógico, los sistemas de inteligencia artificial que son estudiados en el presente trabajo emplean muchos datos de carácter personal para analizar el comportamiento humano. Es por ello que, hasta la fecha, el marco jurídico en materia de protección de datos personales ha servido como principal herramienta para lidiar con los múltiples riesgos derivados del creciente uso de sistemas automatizados. Sin embargo, dicho marco jurídico adolece de importantes deficiencias que a continuación se señalan de manera breve.

El marco jurídico en materia de protección de datos está diseñado para proteger un derecho muy concreto, el derecho a la protección de datos personales. Es por ello que, si bien instrumentos como el Reglamento General de Protección de Datos (en adelante RGPD) [14], señalan también los riesgos que los sistemas de procesamiento de datos pueden generar, por ejemplo, para el derecho a la no discriminación, lo cierto es que, no se establecen mecanismos específicamente dirigidos para proteger frente a todos los riesgos generados por la inteligencia artificial.

Asimismo, el marco jurídico en materia de protección de datos se articula desde una perspectiva de autodeterminación informativa. Esto es, basa el procesamiento en el consentimiento de las personas interesadas y establece un catálogo de derechos que las personas sometidas a tratamientos de datos pueden ejercitar para proteger sus intereses y que incluyen la posibilidad de rectificar sus datos o solicitar información relativa al procesamiento. Sin embargo, esta aproximación no ha generado un sistema efectivo de control, entre otras razones, porque las personas sometidas a procesos de tratamiento de datos no perciben los riesgos de dicho tratamiento de manera directa y porque para muchas personas, especialmente aquellas en situaciones más vulnerables, ejercitar los derechos subjetivos que ofrece por ejemplo el RGPD puede resultar enormemente costoso[15].

---

[13] O'NEIL, Cathy (2017:70).

[14] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[15] HUERGO LORA, Alejandro, (2020): "Una aproximación a los algoritmos desde el Derecho administrativo", en HUERGO LORA, Alejandro (dir.) y DÍAZ GONZÁLEZ, Gustavo Manuel (coord.), *La Regulación de los Algoritmos*, Cizur Menor, Aranzadi, 2020, págs. 56-58; KOOPS, Bert-Jaap, (2014): "The problem with European data protection law", *International Data Privacy Law*, vol. 4, nº 4, pág. 252.

Por otra parte, los mecanismos generales de control que establece el ordenamiento jurídico en materia de protección de datos distan de ser efectivos en la prevención y control de la inteligencia artificial. Esto se debe, en parte, a que normas jurídicas como el RGPD o la Directiva 2016/680[16] no fueron en realidad diseñadas únicamente para regular el procesamiento automatizado de datos personales sino toda clase de procesamiento (automatizado o no) de dicha información.

Por otra parte, cabe destacar que el RGPD está, en realidad, diseñado desde una perspectiva jurídico-privada y las obligaciones y el sistema de control que establece han demostrado ser insuficientes para fiscalizar el uso de sistemas algorítmicos por parte de las Administraciones públicas[17]. Es más, bajo el paraguas del marco jurídico en materia de protección de datos estas han tratado de eludir las obligaciones de transparencia que les son de aplicación.

Finalmente, cabe destacar que, hasta la fecha, la posible solución alternativa que podría tener lugar al aplicar de manera combinada diferentes marcos jurídicos (por ejemplo, en materia de transparencia o igualdad) para lidiar de manera conjunta con los riesgos generados por los sistemas de inteligencia artificial tampoco se ha puesto a prueba. En todo caso, teniendo en cuenta la creciente importancia que tiene la automatización en toda clase de procesos, la creciente capacidad computacional, los riesgos que genera y las particularidades propias de estos sistemas, resulta necesario desarrollar un marco jurídico específico aplicable a la inteligencia artificial.

III. LA PROPUESTA DE REGLAMENTO DE INTELIGENCIA ARTIFICIAL (EN GENERAL)

1. Estructura

La propuesta de Reglamento se estructura en 12 títulos. El primer título (artículos 1 a 4) establece las disposiciones generales, que incluyen el objeto, ámbito de aplicación y

[16] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[17] BOIX PALOP, Andrés (2020a): "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones", *Revista de Teoría y Método*, vol. 1, págs. 223-270; BOIX PALOP, Andrés (2020b): "Algorithms as regulations: considering algorithms, when used by the public administration for decision-making, as legal norms in order to guarantee the proper adoption of administrative decisions", *European Review of Digital Administration & Law*, vol 1, nº 1-2, págs. 75-100.

definiciones, así como la posibilidad de modificar la definición de sistemas de inteligencia artificial que da el anexo I de la propuesta.

El segundo título (artículo 5) establece los sistemas de inteligencia artificial prohibidos. El tercer título (artículos 6 a 51) se centra en los sistemas de inteligencia artificial de alto riesgo, estableciendo los requisitos con los que dichos sistemas deben cumplir, así como las obligaciones y sistemas de control que son de aplicación a los diferentes operadores[18] de sistemas de alto riesgo. El tercer título se ocupa también de regular las entidades encargadas de controlar y supervisar los sistemas de inteligencia artificial.

El Título IV (art. 52) se ocupa de las obligaciones de transparencia aplicables a determinados sistemas, como por ejemplo, los que generan contenidos manipulados en vídeos que parecen reales, esto es, '*deep fake*' o 'ultrafalsificaciones'. El título V (arts. 53 a 55) establece medidas de apoyo a la innovación.

El título VI (arts. 56 a 59) establece las autoridades del nuevo sistema de gobernanza de la inteligencia artificial. El título VII (art. 60) establece la regulación básica para la creación de una base de datos a nivel europeo en el que consten los sistemas de alto riesgo independientes.

El título octavo (arts. 61 a 68) establece las normas para el seguimiento posterior a la comercialización, intercambio de información sobre incidentes y fallos de funcionamiento y vigilancia del mercado. El título noveno (art. 69) regula los códigos de conducta voluntarios.

[18] El art. 3 de la propuesta de Reglamento de Inteligencia Artificial engloba bajo el término "operador" a proveedores, usuarios, representantes autorizados, importadores y distribuidores, que, como se detalla a continuación, son todos aquellos sujetos que, en un momento u otro del proceso de desarrollo y puesta en funcionamiento de los sistemas de inteligencia artificial, deberán asegurar que el sistema cumple con los requisitos fijados por la propuesta de Reglamento y someterse a los procedimientos de control correspondientes: "2) «Proveedor»: toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita; 3) «Proveedor a pequeña escala»: todo proveedor que sea una microempresa o una pequeña empresa en el sentido de la Recomendación 2003/361/CE de la Comisión; 4) «Usuario»: toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional; 5) «Representante autorizado»: toda persona física o jurídica establecida en la Unión que haya recibido el mandato por escrito de un proveedor de un sistema de IA para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor; 6) «Importador»: toda persona física o jurídica establecida en la Unión que introduzca en el mercado o ponga en servicio un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida fuera de la Unión; 7) «Distribuidor»: toda persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercializa un sistema de IA en el mercado de la Unión sin influir sobre sus propiedades."

El título X (arts. 70 a 72) se ocupa del régimen sancionador y establece también una serie de obligaciones de confidencialidad que son de aplicación a las entidades encargadas de controlar los sistemas de inteligencia artificial.

En diversos preceptos de la propuesta de Reglamento se delega a la Comisión Europea el poder de dictar actos de ejecución del Reglamento o de modificar determinadas partes de la regulación contenida en la propuesta normativa con el objetivo de adaptarla a la cambiante realidad de la inteligencia artificial que resulta del progreso tecnológico. La regulación de dicha delegación se establece en el título XI (arts. 73 y 74).

Finalmente, el título XII (arts. 75 a 85) establece las disposiciones finales. La mayor parte de las disposiciones finales se refieren a

2. Ámbito de aplicación

2.1. *Objetivo*

El objeto de la propuesta de Reglamento de Inteligencia Artificial es, evidentemente, regular los sistemas de inteligencia artificial. La definición de sistema de inteligencia artificial puede extraerse del contenido del artículo 3.1 en combinación con lo dispuesto en el anexo I[19] de la propuesta de Reglamento e incluye, tanto los sistemas más avanzados y que, en sentido estricto, sí pueden considerarse "Inteligencia Artificial", como otros sistemas más sencillos que no se caracterizan por su capacidad de autoaprendizaje.

Asimismo, resulta relevante destacar que la propuesta no se ocupa únicamente de aquellos procesos plenamente automatizados, sino también de los usos de sistemas de inteligencia artificial en contextos en los que también intervienen personas. De esta manera se completa el contenido de los arts. 22 #(§037364) ar. 22# RGPD y 11 de la Directiva 2016/680 #(§037365)#, en virtud de los cuales se reconoce la prohibición de tomar decisiones basadas "únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en [la persona interesada] o le afecte significativamente de modo similar".[20]

---

[19] "Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo.

Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico).

Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización".

[20] COTINO HUESO, Lorenzo *et al.* (2021): "Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (*Artificial Intelligence Act*)", *Diario La Ley*, 2 de julio, pág. 6.

2.2. *Subjetivo y territorial*

La propuesta de Reglamento es aplicable a los proveedores de sistemas de inteligencia artificial en todas sus fases, desde el desarrollo inicial hasta la gestión una vez han sido puestos en marcha siempre que el sistema se introduzca en el mercado o ponga en servicio en la UE. También se aplica a los usuarios de sistemas de inteligencia artificial que se encuentren en la UE y a proveedores y usuarios que se encuentren en un tercer país, cuando la información generada por el sistema se emplee en el territorio de la UE.

Esta norma no establece un sistema de derechos subjetivos sino que parece que su principal objetivo es suplir las deficiencias de las herramientas de gobernanza y control general establecidas por el RGPD. Así, la propuesta de reglamento no se refiere en ningún caso a los derechos de las personas afectadas por el uso de sistemas automatizados. Esta es una deficiencia importantísima ya que los derechos reconocidos en el marco jurídico de protección de datos son insuficientes para proteger a las personas afectadas de todos los posibles daños que pueden generar los sistemas de inteligencia artificial[21].

3. Un enfoque basado en el riesgo

Tal como indica la propia exposición de motivos de la propuesta de Reglamento, esta "sigue un enfoque basado en los riesgos" [22] que pueden generar los sistemas de inteligencia artificial. Este es el enfoque que se reclamaba por parte de la doctrina y que también se incorporó al Libro Blanco de Inteligencia Artificial de la Comisión Europea[23] y la Opinión de la Comisión de Ética de Datos Alemana de 23 de octubre de 2019[24].

La propuesta de Reglamento establece cuatro clases de requisitos o sistemas de control en función del riesgo generado:

- Sistemas cuyo riesgo es inasumible y quedan, por tanto, prohibidos (Título II)[25];

[21] COTINO HUESO, Lorenzo *et al.* (2021: 3).

[22] Propuesta de Reglamento de Inteligencia Artificial, pág. 7; VEALE, Michael y ZUIDERVEEN BORGESIUS, Frederik, (2021): "Demystifying the Draft EU Artificial Intelligence Act", *Computer Law Review International*, vol. 22, nº 4, págs. 97-112.

[23] COMISIÓN EUROPEA, (2020): "Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza", COM(2020) 65 final, 19 de Febrero, pp. 24-25.

[24] DATENETHIKKOMMISSION, (2019a): "Gutachten der Datenethikkommission"; DATENETHIK-KOMMISSION, (2019b): "Opinion of the Data Ethics Commission: Executive Summary".

[25] En primer lugar, quedan prohibidos los sistemas empleados con el objetivo de manipular a seres humanos de modo que causen o puedan causar "perjuicios físicos o psicológicos a esa

- Sistemas que generan un alto riesgo y que son objeto de una amplísima regulación (Título III);

- Sistemas que, sin ser considerados de alto riesgo, por sus especiales particularidades deben cumplir con una serie de obligaciones de transparencia más intensas que los sistemas que generan un nivel menor de riesgos (título IV);

- Los restantes sistemas, para cuyo uso únicamente se prevé la posibilidad de establecer códigos de conducta voluntarios (título IX).

IV. LA REGULACIÓN DE LOS SISTEMAS DE ALTO RIESGO

1. La clasificación de los sistemas de alto riesgo

Como resulta lógico, la mayor parte de la propuesta de Reglamento se dedica a regular los sistemas de alto riesgo. De conformidad con la propia exposición de motivos de la propuesta de Reglamento los sistemas de alto riesgo "para la salud y la seguridad o los derechos fundamentales de las personas físicas"[26]. Estos pueden ser clasificados en dos grupos.

Por una parte, el primer grupo comprende aquellos sistemas que, en sí, constituyen los productos o son empleados como componentes de seguridad de determinados productos. Estos productos pueden ser, bien aquellos contemplados en la legislación de armonización que señala el anexo II de la propuesta de Reglamento, bien aquellos que deben "someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio" (art. 6.1.a y b y anexo II).

Sin embargo, teniendo en cuenta que el presente trabajo se centra en aquellos sistemas empleados en el análisis del comportamiento humano y la realidad social, nos centraremos en el segundo grupo de sistemas de inteligencia artificial de alto riesgo, que son los incluidos en el anexo III de la propuesta de Reglamento. Estos son los sistemas empleados 1) para la identificación biométrica y categorización de personas físicas; 2) en el ámbito de la gestión y funcionamiento de infraestructuras esenciales; 3) en contextos

---

persona o a otra" (art. 5.1.a y b). El apartado (a) se refiere al uso de "técnicas subliminales que trasciendan la conciencia de una persona" mientras que el apartado (b) hace referencia a los sistemas que aprovechen "alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental". En segundo lugar, quedan prohibidos los sistemas de crédito social que generen perjuicios para las personas en contextos que no guarden relación con aquellos en los que se generaron o recogieron los datos o que generen un trato perjudicial desproporcionado (art. 5.1.c). Finalmente se prohíbe el uso, con algunas salvedades, de "identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley" (art. 5.1.d).

[26] Propuesta de Reglamento de Inteligencia Artificial, p. 15.

educativos y de formación profesional; 4) en el ámbito del empleo; 5) para determinar y gestionar el acceso y disfrute de servicios públicos y privados esenciales y sus beneficios; 6) en asuntos relacionados con la aplicación de la ley; 7) en la gestión de la migración, el asilo y el control fronterizo y 8) en la administración de justicia y procesos democráticos.

Algunos de los sistemas identificados como sistemas de alto riesgo coinciden con aquellos contextos en los que, en los últimos años, han salido a la luz supuestos específicos de afectación a los derechos fundamentales de las personas. Por ejemplo, en el ámbito del empleo podemos citar el famoso caso del algoritmo desarrollado por Amazon que discriminaba contra las mujeres candidatas a puestos de trabajo en la empresa[27].

Los sistemas enumerados en el anexo III constituyen un *numerus clausus*. Si bien es cierto que el art. 7 de la propuesta permite a la Comisión modificar dicho listado, lo cierto es que esa modificación únicamente puede venir referida a la inclusión de sistemas dentro de los ámbitos ya especificados en el anexo III. Es decir, no es posible añadir nuevos ámbitos en los que se considere que el uso de sistemas de inteligencia artificial generan riesgos altos para la salud, seguridad o derechos fundamentales de las personas. Esta cuestión es problemática por cuanto que actualmente estamos asistiendo a un creciente y constante desarrollo tecnológico lo que dificulta la posibilidad de identificar todos aquellos ámbitos en los que el uso de inteligencia artificial puede generar riesgos significativos. Es más, hay determinados ámbitos que no se incluyen en el listado del anexo III que ya son susceptibles de causar riesgos importantes para la salud, seguridad y derechos fundamentales de las personas. Este es el caso de los sistemas empleados en el contexto sanitario que, tal como apuntan COTINO HUESO *et al.*, no siempre serán empleados como componentes de seguridad de los productos incluidos en el anexo II, ni constituirán dichos productos en sí[28]. Es por ello que sería recomendable establecer una cláusula más flexible de modificación y ampliación de los sistemas contenidos en el anexo III.

1.1. *El problema de los sistemas empleados por las grandes plataformas digitales*

Las grandes empresas tecnológicas como Alphabet (Google), Amazon y Meta (Facebook) emplean muchas clases de sistemas de inteligencia artificial con diferentes propósitos. Cuando las personas interactúan con las plataformas digitales operadas por

[27] DASTIN, Jeffrey, (2018): "Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters,* 10 de octubre. Disponible el 12 de Octubre de 2021 en: https://www.reuters.com/

[28] COTINO HUESO, Lorenzo *et al.* (2021: 6).

dichas empresas el contacto con dichos sistemas es constante. Sin embargo, los sistemas automatizados que emplean las grandes plataformas digitales no se encuentran comprendidos en el listado del anexo III.

Hasta cierto punto, podría argumentarse que dichos sistemas podrían llegar a considerarse comprendidos entre aquellos empleados en el ámbito del "acceso y disfrute de servicios públicos y privados esenciales y sus beneficios". Así, resulta innegable que, en la medida en la que cada vez más interacciones personales y profesionales tienen lugar en el mundo digital, estas empresas operan espacios en los que se ofrecen servicios de carácter esencial para la vida diaria de muchas personas[29]. Es más, como consecuencia de la pandemia del coronavirus, el papel que ocupan dichas plataformas en la vida diaria de las personas ha aumentado de manera exponencial y, si bien es cierto que el uso normal que se realiza actualmente de estos servicios no es el mismo que durante el confinamiento, también lo es que la pandemia ha acelerado la digitalización de la sociedad. Sin embargo, teniendo en cuenta que dichos sistemas no se mencionan de manera explícita en el anexo III, parece evidente que no existe intención alguna de incluirlos como sistemas de alto riesgo. En este sentido, conviene destacar que la única referencia a sistemas empleados por el sector privado en el ámbito del acceso y disfrute de servicios son los "sistemas de IA destinados a utilizarse para evaluar la solvencia de personas físicas o establecer su calificación crediticia".

La razón por la que no se considera que estos sistemas generen un alto riesgo para la salud, seguridad y derechos fundamentales de las personas es, probablemente, que no se percibe que plataformas como Amazon, Google o Facebook, afecten de manera directa o muy significativa a las personas que interactúan con ellas. Esta idea no puede hallarse más lejos de la realidad si analizamos el papel que los servicios de las empresas mencionadas tienen sobre los seres humanos. Estas empresas actúan como monopolios *de facto* en los espacios que ocupan y han sido investigadas y, en algunos casos, multadas por sus prácticas anticompetitivas tanto en los Estados Unidos como en la Unión Europea[30]. El poder monopolístico otorga a estas plataformas la capacidad de

---

[29] SORIANO ARNANZ, Alba, (2021a): *Data Protection of the Prevention of Algorithmic Discrimination. Protecting from discrimination and other harms caused by algorithms through privacy in the EU: possibilities, shortcomings and proposals*, Cizur Menor, Thomson Reuters – Aranzadi, pág. 221.

[30] COMISIÓN EUROPEA, "Defensa de la competencia: la Comisión impone una multa a Google de 1,49 miles de millones de euros por prácticas abusivas en la publicidad en línea", 20 de marzo de 2019. Disponible el 8 de diciembre de 2020 en: https://ec.europa.eu/; FEDERAL TRADE COMISSION, (2021): "FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate". Disponible el 1 de octubre de 2021 en: https://www.ftc.gov/; NADLER, Jerrold y CICILLINE, David, (2020): "Investigation of competition in digital markets", Subcommittee on antitrust, commercial and administrative law of the Committee on the judiciary.

ejercer un verdadero poder regulador sobre aquellos segmentos de los servicios digitales que controlan[31] y de crear arquitecturas de elección con el objetivo de manipular el comportamiento de las personas usuarias[32].

Así, teniendo en cuenta el poder real que tienen estas grandes empresas, sería conveniente establecer una regulación especialmente intensa en lo que a los sistemas de inteligencia artificial que emplean se refiere.

2. Requisitos de los sistemas de alto riesgo y obligaciones de los operadores.

2.1. *Requisitos*

El capítulo segundo del título tercero de la propuesta de Reglamento (arts. 8 a 15) se ocupa de los requisitos que son de aplicación a los sistemas de alto riesgo.

2.1.1. Sistema de gestión de riesgos

Entre estos requisitos cabe destacar, en primer lugar, la necesaria implantación de un sistema de gestión de riesgos para los sistemas de alto riesgo. Conviene indicar que, si bien esta medida se encuentra comprendida entre los requisitos de los sistemas, parece más bien corresponder al ámbito de las obligaciones de los operadores, las cuales se regulan en el capítulo tercero del título tercero. En cualquier caso, el objetivo del establecimiento de dicho sistema de gestión de riesgos es evaluar, a lo largo de todo el periodo de funcionamiento del sistema, los posibles riesgos que puede generar, así como el establecimiento de medidas para mitigar aquellos. Esta obligación se configura más bien como el marco o directrices generales dentro de las cuales se desarrollan los restantes requisitos y obligaciones aplicables a los sistemas de alto riesgo y no tanto como una serie de instrucciones específicas de acción.

2.1.2. Datos y gobernanza de datos

Muchos de los problemas generados por sistemas algorítmicos son el resultado de las bases de datos con las que dichos sistemas son entrenados. Por ejemplo, muchos

[31] KIM, Nancy y TELMAN, Jeremy, (2015): "Internet giants as quasi-governmental actors and the limits of contractual consent", *Missouri Law Review*, vol. 80, nº 3, págs. 723-770.

[32] YEUNG, Karen, (2017): "'Hypernudge': Big data as a mode of regulation by design", *Information, Communication & Society*, vol. 20, nº 1, págs. 118-136; HEMPPHILL, Thomas, A. y BANERJEE, Syagnik, (2021): "Facebook and sef-regulation: efficacious proposals – or 'smoke and mirrors'?", *Technology in Society*, nº 67, págs. 1-6.

supuestos de discriminación algorítmica son el resultado de emplear bases de datos que infra- o sobrerrepresentan a determinados grupos de la población[33].

La infrarrepresentación de un grupo poblacional en una base de datos puede deberse a su falta de acceso a la tecnología o a supuestos históricos de discriminación. Tomemos por ejemplo el caso de los ascensos. Si se introducen datos históricos sobre ascensos en el programa informático diseñado para indicar qué características son más comunes en las personas que han sido ascendidas en el pasado, la mayoría de los sujetos que aparecen en el conjunto de datos serán hombres[34].

También es posible que la sobrerrepresentación de un grupo concreto dé lugar a situaciones de discriminación. Por ejemplo, digamos que en una ciudad se ha producido un mayor grado de detenciones en un determinado barrio debido a que está mayoritariamente poblado por personas migradas. La cantidad desproporcionada de detenciones de personas migradas (que en muchas ocasiones pertenecen también a una minoría racial) probablemente derivará en que, por ejemplo, las personas procedentes de Latinoamérica o África que hayan cometido delitos sean detenidas con una frecuencia mucho mayor que aquellos nacionales que hayan cometido algún delito. En consecuencia, si los sujetos cuyos datos aparecen en el conjunto de datos de entrenamiento son exclusivamente personas que han sido detenidas o condenadas anteriormente, al introducir los datos en el algoritmo, éste extraerá una relación relevante entre ser una persona migrada y cometer un delito. Este es precisamente el problema que se ha planteado con respecto a ciertas herramientas de predicción empleadas por las fuerzas y cuerpos de seguridad[35].

En otras ocasiones los daños que se pueden ocasionar por el uso de sistemas de inteligencia artificial y que se derivan de la base o bases de datos empleadas son el resultado de los errores que estas contienen. Sobre todo es importante resaltar que es más frecuente la existencia de errores que afecten a las personas pertenecientes a grupos desaventajados, lo que contribuye, una vez más, a perpetuar la desigualdad a través de la automatización de procesos decisorios[36].

Con el objetivo de abordar los riesgos que puedan derivarse de los datos empleados en el entrenamiento de modelos algorítmicos, el art. 10 de la propuesta de Reglamento

---

[33] BAROCAS, Solon y SELBST, Andrew, (2016): "Big data's disparate impact", *California Law Review*, vol. 104, nº. 3, pág. 681.

[34] DATTA, Anupam *et al.* (2017): "Proxy non-discrimination in data-driven systems: theory and experiments with machine learnt programs", p. 1. Disponible el 15 de septiembre de 2021 en: https://arxiv.org/

[35] BAROCAS, Solon y SELBST, Andrew, (2016: 681).

[36] KIM, Pauline, (2017): "Data-driven discrimination at work", *William & Mary Law Review*, vol. 58, págs. 885-886.

establece una serie de requisitos que son de aplicación a los datos empleados en los procesos de entrenamiento, validación y prueba de los sistemas algorítmicos. Con el objetivo de garantizar que los conjuntos de datos carezcan de errores, sean pertinentes, representativos y estén completos, se establecen una serie de prácticas de gobernanza que deben cumplir los proveedores[37]. Estas obligaciones incluyen el examen de posible sesgos, la detección de lagunas y la elección del diseño adecuado, entre otras.

Uno de los aspectos más relevantes de este precepto es la excepción que fija en relación con el art. 9 #(§037364) ar. 9# del RGPD y 10 de la Directiva 2016/680 #(§037365)#. Dichos preceptos establecen la prohibición general de tratar los datos que revelen "el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical" de una persona física así como "el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

Dicha prohibición ha sido criticada por la doctrina en la medida en que puede dificultar la detección de supuestos de discriminación algorítmica ya que la no inclusión de las categorías de datos especiales no implica que el sistema no sea capaz de inferirlas de otra información y conducir así a la toma de decisiones discriminatorias[38]. Es por ello que la adopción de esta excepción con el objetivo de detectar y corregir sesgos contenidos en el sistema debe ser valorada de manera muy positiva.

Por último, este precepto sirve también como mecanismo para subsanar algunas deficiencias derivadas de la aproximación desde la autodeterminación informativa que realiza el RGPD a la protección de datos personales. Así, el art. 16 #(§037364) ar. 16# del RGPD, al establecer el derecho de rectificación, ofrece a las personas interesadas en el tratamiento la posibilidad de solicitar que se completen sus datos personales que sean incompletos. Sin embargo, hacer la responsabilidad de protegerse frente a los riesgos generados por los tratamientos de datos recaiga plenamente en los individuos puede generar deficiencias en el control efectivo de los sistemas algorítmicos pues no garantiza

[37] Si bien no se especifica quiénes son los sujetos obligados a realizar las prácticas de gobernanza de datos establecidas en el art. 10.2 se sobreentiende que serán los proveedores, esto es, los desarrolladores del sistema, ya que las tareas a las que se refiere dicho precepto tendrán lugar en el momento de desarrollar el sistema. Asimismo, el art. 10.5 sí menciona a los proveedores cuando excepciona la prohibición de analizar las categorías especiales de datos del artículo 9 del RGPD para la detección y corrección de sesgos. Por consiguiente, consideramos que debe entenderse que las restantes obligaciones recogidas en el art. 10 se refieren también a los proveedores.

[38] GOODMAN, Bryce, (2016): "A step towards accountable algorithms?: Algorithmic discrimination and the European Union general data protection", trabajo presentado en la *29th Conference on Neural Information Processing Systems*, Barcelona, 2016, pág. 3. Disponible el 10 de octubre de 2021 en: http://www.mlandthelaw.org/

que los derechos vayan a ser ejercitados por todas las personas sometidas a tratamientos de datos[39]. Por ello, el establecimiento de una serie de requisitos que deben cumplir las bases de datos empleadas para el entrenamiento, validación y prueba de los modelos y que deben asegurarse por los propios proveedores (desarrolladores) de los sistemas, sin duda contribuye a completar algunas de las carencias del marco jurídico en materia de protección de datos.

2.1.3. *Requisitos relacionados con la transparencia, explicabilidad y comprensibilidad de los sistemas*

Como ya se ha indicado anteriormente, uno de los principales problemas que se derivan del creciente uso de sistemas de inteligencia artificial, sobre todo en aquellos contextos en los que son empleados para analizar y predecir el comportamiento humano y la realidad social, es su opacidad. Esta falta de transparencia dificulta el control de los sistemas algorítmicos. Por tanto, la propuesta de "Ley de Inteligencia Artificial" europea trata de establecer una serie de requisitos con los que deben de cumplir los operadores de los sistemas con el objetivo de aumentar las posibilidades de control de los sistemas de inteligencia artificial.

El art. 11 de la propuesta de reglamento establece la obligación de preparar y mantener actualizada la documentación técnica relativa al sistema. El contenido de dicha documentación técnica se detalla en el anexo IV de la propuesta. Dicha documentación deberá incorporar información bastante detallada relativa a la configuración y funcionamiento del sistema. El cumplimiento de este requisito facilitará el control general de los sistemas de inteligencia artificial, no solo por las autoridades competentes sino por los propios desarrolladores que se verán obligados a examinar los sistemas de manera extensiva para elaborar la documentación técnica. Ahora bien, para que este requisito contribuya verdaderamente a mejorar la fiscalización de los sistemas de inteligencia artificial de alto riesgo resulta necesario que su cumplimiento no sea meramente formal.

También se establece la obligación de registrar las acciones del sistema. Esta obligación resulta especialmente relevante si atendemos a los sistemas que son capaces de desarrollarse de manera autónoma incluso tras su puesta en marcha. En este sentido, se ha destacado, por ejemplo, la dificultad de aportar pruebas o elementos de comparación en los supuestos de discriminación algorítmica en los que el sistema empleado modifica constantemente los parámetros de análisis que emplea[40]. A través

[39] SORIANO ARNANZ, Alba (2021a: 218-225).

[40] SORIANO ARNANZ, Alba, (2021b): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, nº 56, pág. 18.

del registro de eventos del sistema se podrá trazar la lógica empleada en cada momento para poder asegurar la fase de prueba en los procesos en que se juzguen supuestos de discriminación algorítmica pero también aquellos en los que se trate de acreditar la ilegalidad de la decisión total o parcialmente automatizada.

El art. 13 de la propuesta se refiere a la "transparencia y comunicación de información a los usuarios". Como ya se ha indicado anteriormente, la norma no establece un sistema de derechos individuales que puedan ejercitar las personas sometidas a procesos en los que se vean afectadas por sistemas de inteligencia artificial. Así, cuando el reglamento se refiere a "usuarios", dicho término comprende a "toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional". La transparencia y comunicación de información exigidas en este precepto se refieren, por tanto, a la información necesaria para que los usuarios, como operadores del sistema, sean también conscientes de los riesgos que este puede llegar a generar y puedan así prevenir y controlarlos.

2.1.4. *Intervención humana*

Desde una perspectiva teórica, la intervención de un ser humano en un proceso decisorio en el que se empleen sistemas de inteligencia artificial, responde a la necesidad de no deshumanizar a las personas que son sometidas a procesos automatizados de tratamiento de datos. Reconocer el derecho a que una persona analice y supervise las decisiones tomadas por "la máquina" implica reconocer el derecho de los sujetos del tratamiento a no ser tratadas como objetos[41]. Desde una perspectiva más práctica, la intervención humana aporta al proceso decisorio un grado de empatía del que carecen los sistemas de inteligencia artificial, garantizando así que las particularidades de cada sujeto son analizadas y tenidas en cuenta y que, por tanto, se respeta el debido proceso tecnológico[42].

La intervención o supervisión por parte de seres humanos de los sistemas automatizados de tomad de decisiones no es una novedad. El art. 22 #(§037364) ar. 22# RGPD establece el derecho a la intervención humana como medida de protección en aquellos casos en los que se excepciona la prohibición de "ser objeto de una decisión

[41] JONES, Meg Leta, (2017): "The right to a human in the loop: Political constructions of computer automation and personhood", *Social Studies of Science,* vol. 47, nº 2, págs. 231-232

[42] PONCE SOLÉ, Juli, (2019): "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, nº 50, págs. 28-33; RANCHORDÁS, Sofia, (2022): "Empathy in the digital administrative State", *Duke Law Review*, vol. 72, en prensa. Disponible el 20 de octubre de 2021 en: https://papers.ssrn.com/

basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles". Lo que hace la nueva normativa es ampliar el detalle con el que se regulan las posibilidades que puede ofrecer este mecanismo de salvaguarda, atendiendo a cuestiones problemáticas como el "sesgo de automatización", esto es, la tendencia de los seres humanos a confiar en la corrección de los resultados ofrecidos por los sistemas de inteligencia artificial[43].

Sin embargo, este precepto da libertad a los proveedores para decidir la forma en que se articulará este mecanismo, no estableciendo si quiera qué se considera una suficiente intervención humana. Es decir, por una parte, recoge de manera mucho más completa que el RGPD la forma en que se podría articular la supervisión humana y las cuestiones que se podrían tener en cuenta al establecer este mecanismo, pero no fija ningún mandato específico más allá de la obligación genérica de intervención humana.

2.2. *Obligaciones de los operadores*

Las obligaciones de los operadores se establecen en los arts. 16 a 29 de la propuesta de Reglamento y se refieren, fundamentalmente, a aquellas actividades que deben ser desarrolladas con el objetivo de garantizar, por una parte, que los sistemas de inteligencia artificial de alto riesgo cumplen con los requisitos fijados en el capítulo segundo del título tercero (examinados en el apartado anterior) y, por otra parte, la efectividad de los sistemas de control que fija la propuesta normativa.

Con respecto a los proveedores, es decir, los desarrolladores de los sistemas, estos deben velar por que los sistemas cumplan con los requisitos del capítulo dos del título tercero; establecer un sistema de gestión de la calidad para asegurar que el sistema cumple con lo dispuesto en el Reglamento; elaborar la documentación técnica; conservar los archivos de registro que estén bajo su control; adoptar las medidas correctoras necesarias para que el sistema cumpla con los requisitos que fija el Reglamento; informar a las autoridades cuando un sistema que hayan comercializado o puesto en servicio no cumpla con algún requisito y colocar el marcado CE en los sistemas de inteligencia artificial.

Además, los proveedores son también los operadores encargados de llevar a cabo la evaluación de conformidad, de demostrar, a solicitud de la autoridad nacional competente, que sus sistemas de inteligencia artificial de alto riesgo cumplen los requisitos del capítulo dos del título tercero de la propuesta de Reglamento y registrar los sistemas de alto riesgo en el registro correspondiente. Estas obligaciones se analizan de

[43] CITRON, Danielle Keats, (2008): "Technological due process", *Washington University Law Review*, vol. 85, nº 6, págs. 1271-1272.

manera separada en los dos próximos apartados del presente trabajo por su relevancia como mecanismos de control de los sistemas de inteligencia artificial.

Las obligaciones de los restantes operadores se centran en asegurar que el proveedor ha cumplido con la obligación de elaborar la documentación técnica, colocar el marcado CE y ha realizado la evaluación de conformidad. Los usuarios deben asegurarse de emplear el sistema de conformidad con las instrucciones dadas por el proveedor. Es decir, las obligaciones están configuradas de manera que aseguran que todos los agentes que intervienen en el proceso de desarrollo, distribución y utilización del sistema ejercen alguna función de control.

3. Autoridades de control y evaluación de la conformidad

Durante los últimos años se ha venido reclamando el establecimiento de autoridades independientes encargadas de controlar el uso de sistemas de inteligencia artificial[44]. Este es el papel que se otorga, parcialmente, a las autoridades notificantes reguladas en el art. 30 de la propuesta de reglamento. Sin embargo, no son estas las encargadas de desarrollar el principal mecanismo de control *ex ante* de los sistemas de inteligencia artificial, la evaluación de la conformidad del art. 43.

Se prevé así el establecimiento de una red de organismos notificados (art. 33), equivalentes a autoridades certificadoras que se encargarán de evaluar que los sistemas de inteligencia artificial cumplen con los requisitos del capítulo dos del título tercero de la propuesta de reglamento. Entre las muchas limitaciones que puede comportar este sistema por la posible falta de independencia de los organismos notificados[45], conviene destacar que la intervención de los organismos notificados ni siquiera es necesaria para la mayor parte de sistema de inteligencia artificial del anexo III. Así, el art. 43.2 de la propuesta de reglamento se establece que para los supuestos 2 a 8 del anexo III, la evaluación de conformidad se fundamentará en un control interno, esto es, será el propio proveedor quien compruebe que el sistema cumple con los requisitos establecidos en la norma.

Así, si bien es cierto que las autoridades notificantes pueden solicitar la información relativa al sistema, la ausencia de intervención de un tercero en el mecanismo *ex ante* de

[44] SCHERER, Matthew, (2016): "Regulating artificial intelligence systems: risks, challenges, competencies, and strategies", *Harvard Law & Technology Journal*, vol. 29, nº 2, págs. 353-400; TUTT, Andrew, (2017): "An FDA for algorithms", *Administrative Law Review*, vol. 69, nº 1, págs. 83-123; VELASCO RICO, Clara, (2019): "Vigilando al algoritmo. Propuestas organizativas para garantizar la transparencia", en PUENTES COCIÑA, Beltrán y QUINTIÁ PASTRANA, Andrei (dirs.), *El Derecho ante la Transformación Digital*, Barcelona, Atelier, págs. 81-82.

[45] EDWARDS, Lilian y VEALE, Michael, (2018): "Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?", *IEEE Security & Privacy*, vol. 16, nº 3, pág. 52.

control genera serias dudas acerca de la verdadera efectividad de la propuesta normativa.

4. Una base de datos para sistemas de alto riesgo independientes

El Título VII (art. 60) indica que se creará una base de datos que contendrá la información relativa a los sistemas de Inteligencia Artificial del Anexo III. Este mecanismo debe valorarse muy positivamente por cuanto que facilitará la eliminación de la opacidad que existe en relación con el uso de sistemas de inteligencia artificial, proporcionando un mecanismo para el control y la defensa de los derechos de las personas afectadas por dichos sistemas.

V. CONCLUSIONES FINALES

El presente trabajo ha realizado un breve y general repaso por algunos de los aspectos contenidos en la propuesta de reglamento de inteligencia artificial de la UE. La propuesta normativa presenta un marco jurídico insuficiente para hacer frente a los riesgos que se derivan del creciente uso de sistemas de inteligencia artificial. Si bien algunos de los requisitos que deben cumplir los sistemas de inteligencia artificial deben valorarse positivamente, conviene apuntar a la dudosa eficacia de los mecanismos de control fijados en el Reglamento, los cuales se apoyan sobre todo en la actividad de los propios desarrolladores de los sistemas sometidos a control. En definitiva, salvo que la propuesta normativa se modifique considerablemente antes de su aprobación, continuamos con una situación en la que la automatización de procesos afecta de manera cada vez más directa a los derechos de la ciudadanía sin disponer de mecanismos adecuados para prevenir y lidiar con los muchos daños que los sistemas de inteligencia artificial pueden llegar a ocasionar.

VI. BIBLIOGRAFÍA

BAROCAS, Solon y SELBST, Andrew, (2016): “Big data’s disparate impact”, *California Law Review*, vol. 104, nº. 3, pp. 671-732.

- (2018): “The intuitive appeal of explainable machines”, *Fordham Law Review*, vol. 87, nº 3, págs. 1085-1139.

BOIX PALOP, Andrés (2020a): “Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones”, *Revista de Teoría y Método*, vol. 1, págs. 223-270.

- (2020b): “Algorithms as regulations: considering algorithms, when used by the public administration for decision-making, as legal norms in order to guarantee the proper adoption of administrative decisions”, *European Review of Digital Administration & Law*, vol 1, nº 1-2, págs. 75-100.

- (2021): “Digital platforms competition regulatory challenges”, *Revista General de Derecho de los Sectores Regulados*, nº 8.

BURRELL, Jenna “How the machine ‘thinks’: understanding opacity in machine learning algorithms”, *Big Data & Society*, vol. 3, nº 1, 2016, pp. 1-12.

CERRILLO I MARTÍNEZ, Agustí, (2019): “El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?”, *Revista General de Derecho Administrativo*, nº 50, págs. 1-38.

CITRON, Danielle Keats, (2008): “Technological due process”, *Washington University Law Review*, vol. 85, nº 6, págs. 1249-1313.

COGLIANESE, Cary y LEHR, David, (2017): “Regulating by robot: administrative decision making in the machine-learning era”, *The Georgetown Law Journal*, vol. 105, nº 5, págs. 1147-1223.

COMISIÓN EUROPEA, (2019): “Defensa de la competencia: la Comisión impone una multa a Google de 1,49 miles de millones de euros por prácticas abusivas en la publicidad en línea”, 20 de marzo. Disponible el 8 de septiembre de 2021 en: https://ec.europa.eu/

- (2020): “Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza”, COM(2020) 65 final, 19 de Febrero.

COTINO HUESO, Lorenzo; CASTILLO, Juan Antonio; SALAZAR, Idoia; BENJAMINS, Richard; CUMBRERAS, María y ESTEBAN, Adaya María, (2021): “Un análisis crítico constructivo de la Propuesta de Reglamento de la Unión Europea por el que se establecen normas armonizadas sobre la Inteligencia Artificial (*Artificial Intelligence Act*)”, *Diario La Ley*, 2 de julio, págs. 1-15.

DASTIN, Jeffrey, (2018): “Amazon scraps secret AI recruiting tool that showed bias against women”, *Reuters,* 10 de octubre. Disponible el 12 de Octubre de 2021 en: https://www.reuters.com/

DATENETHIKKOMMISSION, (2019a): “Gutachten der Datenethikkommission”.

- (2019b): “Opinion of the Data Ethics Commission: Executive Summary”.

DATTA, Anupam, FREDRIKSON, Matt, KO, Gihyuk, MARDZIEL, Piotr y SEN, Shayak, (2017): “Proxy non-discrimination in data-driven systems: theory and experiments with machine learnt programs”, p. 1. Disponible el 15 de septiembre de 2021 en: https://arxiv.org/

EDWARDS, Lilian y VEALE, Michael, (2018): "Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?", *IEEE Security & Privacy*, vol. 16, nº 3, págs. 46-54.

FEDERAL TRADE COMISSION, (2021): "FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate", 19 de agosto. Disponible el 1 de octubre de 2021 en: https://www.ftc.gov/;

GOODMAN, Bryce, (2016): "A step towards accountable algorithms?: Algorithmic discrimination and the European Union general data protection", trabajo presentado en la *29th Conference on Neural Information Processing Systems*, Barcelona, 2016. Disponible el 10 de octubre de 2021 en: http://www.mlandthelaw.org/

HEMPPHILL, Thomas, A. y BANERJEE, Syagnik, (2021): "Facebook and sef-regulation: efficacious proposals – or 'smoke and mirrors'?", *Technology in Society*, nº 67, págs. 1-6.

HUERGO LORA, Alejandro, (2020): "Una aproximación a los algoritmos desde el Derecho administrativo", en HUERGO LORA, Alejandro (dir.) y DÍAZ GONZÁLEZ, Gustavo Manuel (coord.), *La Regulación de los Algoritmos*, Cizur Menor, Aranzadi, 2020, págs. 23-87.

JONES, Meg Leta, (2017): "The right to a human in the loop: Political constructions of computer automation and personhood", *Social Studies of Science,* vol. 47, nº 2, págs. 216-239.

KAMINSKI, Margot, (2019): "Binary governance: Lessons from the GDPR's approach to algorithmic accountability", *Southern California Law Review*, vol. 92, núm. 6, 2019, págs. 1529-1616.

KIM, Nancy y TELMAN, Jeremy, (2015): "Internet giants as quasi-governmental actors and the limits of contractual consent", *Missouri Law Review*, vol. 80, nº 3, págs. 723-770.

KIM, Pauline, (2017): "Data-driven discrimination at work", *William & Mary Law Review*, vol. 58, págs. 857-936.

KOOPS, Bert-Jaap, (2014): "The problem with European data protection law", *International Data Privacy Law*, vol. 4, nº 4, págs. 250-261.

MESTRE DELGADO, Juan Francisco, (2018): "Una reflexión sobre la regulación constitucional del Derecho administrativo", *Corts: Anuario de Derecho Parlamentario*, nº extra 31, págs. 367-386.

NADLER, Jerrold y CICILLINE, David, (2020): "Investigation of competition in digital markets", Subcommittee on antitrust, commercial and administrative law of the Committee on the judiciary.

NOBLE, Safiya, (2018): *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York University Press, Nueva York.

O'NEIL, Cathy, (2017): *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin Books, Londres.

PONCE SOLÉ, Juli, (2019): "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, nº 50, págs. 1-52.

RANCHORDÁS, Sofia, (2022): "Empathy in the digital administrative State", *Duke Law Review*, vol. 72, en prensa. Disponible el 20 de octubre de 2021 en: https://papers.ssrn.com/

SCHERER, Matthew, (2016): "Regulating artificial intelligence systems: risks, challenges, competencies, and strategies", *Harvard Law & Technology Journal*, vol. 29, nº 2, págs. 353-400.

SORIANO ARNANZ, Alba, (2021a): *Data Protection of the Prevention of Algorithmic Discrimination. Protecting from discrimination and other harms caused by algorithms through privacy in the EU: possibilities, shortcomings and proposals*, Cizur Menor, Thomson Reuters – Aranzadi.

- (2021b): "Decisiones automatizadas y discriminación: aproximación y propuestas generales", *Revista General de Derecho Administrativo*, nº 56, págs. 1-30.

TUTT, Andrew, (2017): "An FDA for algorithms", *Administrative Law Review*, vol. 69, nº 1, págs. 83-123.

VEALE, Michael y ZUIDERVEEN BORGESIUS, Frederik, (2021): "Demystifying the Draft EU Artificial Intelligence Act", *Computer Law Review International*, vol. 22, nº 4, págs. 97-112.

VELASCO RICO, Clara, (2019): "Vigilando al algoritmo. Propuestas organizativas para garantizar la transparencia", en PUENTES COCIÑA, Beltrán y QUINTIÁ PASTRANA, Andrei (dirs.), *El Derecho ante la Transformación Digital*, Barcelona, Atelier, págs. 73-89.

YEUNG, Karen, (2017): "'Hypernudge': Big data as a mode of regulation by design", *Information, Communication & Society*, vol. 20, nº 1, págs. 118-136.

LAS INHERENTES LIMITACIONES DEL MODELO AUTODETERMINISTA DE PROTECCIÓN DE DATOS EN EUROPA

Por

MIREIA ARTIGOT GOLOBARDES
Investigadora Ramón y Cajal Derecho Civil
Universidad Pompeu Fabra

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

RESUMEN: Las políticas de privacidad son un elemento previo e ineludible a cualquier actividad digital. Los individuos pueden aceptar, rechazar o personalizar el acceso a sus datos personales y eventualmente el tratamiento que se pueda realizar con ellos. El modelo europeo de protección de datos se estructura en torno al consentimiento del sujeto: si los individuos tienen información sobre los datos a los que se acceden y al tratamiento que eventualmente se les pueda dar, éstos podrán configurar la política de privacidad de acuerdo con sus preferencias. A pesar de sus buenas intenciones, este modelo está demostrando ser notablemente ineficaz y defectuoso. Este artículo sostiene que la naturaleza de los datos, sus dimensiones colectivas y dinámicas y las limitaciones cognitivas y racionales de los individuos, independientemente de la información que se les proporcione, no hacen posible que éstos puedan evaluar correctamente el contenido de las políticas de privacidad y su potencial impacto para su bienestar futuro en mercados digitales. Para mejorar la eficacia de la protección de datos en Europa deberían adoptarse medidas de derecho público ex ante y ex post.

PALABRAS CLAVE: protección de datos, consentimiento, tratamiento de datos, bienestar del consumidor, limitaciones cognitivas y racionales.

SUMARIO: I. INTRODUCCIÓN. II. LAS POLÍTICAS DE PRIVACIDAD COMO FILTRO A LA ACTIVIDAD DIGITAL. III. EL MODELO AUTODETERMINISTA – AUNQUE NO CONTRACTUAL – DEL RÉGIMEN DE PROTECCIÓN DE DATOS EN EUROPA. 3.1. El concepto de datos personales. 3.2. Mecanismos de acceso y obtención de datos personales. 3.3. El tratamiento de los datos personales. 3.4. Los derechos de los sujetos relativos al acceso y tratamiento de sus datos personales. IV. LAS INHERENTES LIMITACIONES DEL MODELO AUTODETERMINISTA DE PROTECCIÓN DE DATOS. 4.1. La naturaleza de los datos personales. 4.2. La dimensión colectiva y dinámica de los datos personales. 4.3. La dicotomía entre consentimiento y control: asimetría contractual y limitaciones cognitivas de los interesados en el control y gestión de los datos personales. V. ¿UN MODELO DE PROTECCIÓN DE DATOS EMINENTEMENTE PRIVADO O UN MODELO EFECTIVO? VI. CONCLUSIÓN.

ALGORITHMIC CONTRACTING AND THE LIMITS OF CONTRACT LAW

ABSTRACT: Privacy policies are a previous and unavoidable element of digital activity. Individuals can accept, reject or personalize the access to their personal data and eventually the processing that may be done with it. The European model of data protection is structured around the individual's consent: if individuals have information about the data being collected and how it may be

processed they will be able to consent and set the privacy policy according to their preferences. Despite its good intentions, this model is proving to be remarkably ineffective and flawed. This article argues that the nature of data, its collective and dynamic dimensions and the behavioral limitations of individuals do not, regardless of the information provided, allow them to be able to correctly assess the content of privacy policies and its potential impact for their future welfare in online markets. This article argues that in order to enhance the effectiveness of data protection in Europe, ex ante and ex post public law measures should be adopted.

KEYWORDS: data protection, consent, data processing, consumer welfare, behavioral limitations.

I. INTRODUCCIÓN

La protección de datos es uno de los elementos necesarios e imprescindibles para que el desarrollo de los mercados digitales y para que las plataformas sociales garanticen los derechos de los usuarios que participan en ellas.

Los datos personales de los usuarios se encuentran en la antesala de cualquier actividad digital: para poder acceder a un contenido de una página en Internet es necesario previamente haber configurado, aceptado, o rechazado su política de privacidad. La configuración de la política de privacidad por parte de los individuos también es un elemento previo y necesario para poder descargar y poder utilizar una aplicación digital. Así, las políticas de privacidad se configuran como elemento previo, necesario e imprescindible al acceso al contenido digital ya sea en formato de página web o de aplicación ya que determinan los términos en base los cuales se podrá acceder y tratar los datos personales del individuo.

Los datos personales de los individuos no se refieren solamente a aquellos que describen su persona, que también, sino a aquellos que se generan a través de su actividad digital y los que se infieren a través de la agregación de estos datos personales con datos de otros individuos. La actividad online genera una ingente cantidad de información sobre por ejemplo las características de los participantes en mercados multi-cara digitales, sus preferencias, intereses, opiniones, transacciones que llevan a cabo…. Estas variables tanto a nivel individual como a nivel agregado proporcionan información de gran valor para los para los gestores del mercado - sean plataformas prestadoras de servicio, aplicaciones o mercados de doble cara – y para los oferentes porque en base a esta información pueden conocer las preferencias, nivel de renta, lugar de residencia, el tipo de ordenador que se utiliza y la hora en la que el individuo se conecta, entre otros. Además, al combinar esta información personal con los datos personales de individuos directamente con quién nos relacionamos familiar y socialmente es posible dibujar un perfil aún más exacto de nuestras preferencias en base a nuestro comportamiento y decisiones pasadas e inferir nuestras decisiones futuras en el mercado con una sorprendente exactitud.

Esta información es de gran valor para los reguladores, para los gestores de mercados, para los oferentes y para los individuos, particularmente en relación a la personalización de la experiencia digital. Concretamente, los datos personales y el rastro digital del individuo constituyen información muy valiosa para las empresas que ven posible dirigir la publicidad de sus productos a individuos que con elevada probabilidad estuvieran interesados en ellos, personalizar recomendaciones de productos/experiencias y compras y eventualmente personalizar contratos en transacciones con consumidores.

El modelo europeo de protección de datos personales es un modelo autodeterminista en base el cual el individuo se sitúa en el centro y es quién, en base a la información relativa a los datos eventualmente recogidos y de su tratamiento y a sus preferencias configura la política de privacidad y consiente a compartir y/o tratar sus datos personales, rechaza permitir el acceso y/o tratamiento de sus datos o personaliza, como él considera, dicho acceso y tratamiento.

El modelo europeo se estructura alrededor de control de los datos personales por parte del individuo y en su capacidad para realizar una gestión informada en base a sus preferencias y criterio. La idea fundamental del modelo europeo de protección de datos es considerar que, si el individuo dispone de información transparente, podrá autorizar, o no, a través de su consentimiento al acceso y tratamiento de sus datos personales. El modelo europeo, así, tiene un corte privatista claro: los datos personales son objetos de derechos reales – son objeto de propiedad - sobre los cuales el individuo decide en base a su autonomía privada. Si el individuo cuenta con información veraz y transparente respecto al acceso y tratamiento de los datos este se encontrará en una situación óptima para poder gestionar sus datos personales a través de prestar consentimiento – o no - a su acceso y tratamiento.

Este modelo tiene buenas y valiosas intenciones: sitúa al individuo en el centro del régimen jurídico como legitimado para tomar decisiones sobre su privacidad y modularla así según sus preferencias. Sin embargo, la aplicación práctica de este modelo privado y autodeterminista cuestiona, de forma significativa, su eficacia. Las políticas de privacidad diseñadas y redactadas por los predisponentes contienen términos y conceptos técnicos y jurídicos que a menudo requieren un conocimiento por parte de los individuos del que, con frecuencia, no se dispone. De igual forma, los individuos, de forma generalizada, no leen las políticas de privacidad y prestan por lo tanto un consentimiento ignorante. Pero, además, incluso en casos en los cuales los individuos leyeran y pudieran entender el contenido de las políticas de privacidad no resulta posible para los individuos, como consecuencia de la naturaleza de los datos personales, evaluar los efectos de estas en su bienestar tanto presente como futuro.

Este artículo cuestiona el enfoque autodeterminista del modelo europeo de protección de datos en base a tres variables que de forma inherente limitan su eficacia: en primer lugar, la naturaleza de los datos personales no permite a los individuos prestar un consentimiento informado. Segundo, la complejidad del tratamiento de datos incorpora variables colectivas y temporales desconocidas en el momento de prestar consentimiento y tercero, las limitaciones cognitivas y racionales de los individuos no hacen posible, independientemente de la información disponible, realizar una evaluación de los efectos e impacto de las políticas de privacidad en el bienestar presente y futuro del individuo.

La naturaleza del modelo europeo de Protección de Datos y sus limitaciones se presentan en los siguientes apartados.

II. LAS POLÍTICAS DE PRIVACIDAD COMO FILTRO A LA ACTIVIDAD DIGITAL

Los análisis de los mercados digitales, páginas web, redes sociales, plataformas, aplicaciones a menudo se centran en la estructura del mercado en el que participan, el impacto sobre les competidores, las externalidades de red que presentan o las relaciones jurídicas entre los participantes - si tienen una relación laboral o no. Las estructuras digitales de páginas web, plataformas o aplicaciones son muy heterogéneas, las relaciones jurídicas entre sus participantes son de diversa naturaleza y los servicios o actividades digitales que se pueden desarrollar también son muy distintas - desde buscadores, redes sociales hasta mercados de doble cara. Sin embargo, todas ellas comparten una característica esencial: con anterioridad al acceso a las páginas plataformas o aplicaciones digitales es necesario configurar - en forma de aceptación, rechazo o personalización - la política de privacidad de la página web plataforma o aplicación digital. Es decir, la configuración de los datos personales que el individuo permite compartir y eventualmente tratar es un elemento previo y necesario al acceso a la página web, a la plataforma o a la aplicación digital.

Un ejemplo que ilustra esta estructura dual es la contratación con consumidores en mercados digitales. La contratación con consumidores en mercados digitales se estructura en dos partes con elementos y objetos distintos y funcionalmente autónomos, pero íntimamente relacionados. Cuando un consumidor entra en una página web, plataforma, aplicación o mercados de dos caras lo primero en lo que se encuentra es una solicitud para acceder – y eventualmente tratar - sus datos personales de navegación, perfil, teléfono, geolocalización …. así, un elemento imperativo anterior a la transacción con el que se encuentra el consumidor es la solicitud para compartir y eventualmente tratar sus datos personales. El acceso, rechazo o configuración personal respecto al acceso y tratamiento de los datos personales que el consumidor esté dispuesto – o no- a compartir es un primer filtro que determina el estatus presente y eventualmente futuro del

consumidor en el mercado digital en el que tiene por objetivo participar – y eventualmente en mercados en los que en el momento de consentir no imagina que participará.

Una vez aceptado, rechazado o configurado de forma personalizada la política de privacidad, el segundo elemento de la contratación con consumidores en mercados digitales se encuentra en la configuración de la transacción que tiene por objeto el intercambio de bienes y/o servicios en mercados digitales. La regulación de la protección de los consumidores en la Unión Europea es de aplicación a transacciones que tienen lugar en mercados tradicionales, así como mercados digitales. Aunque estructuralmente parecida a la regulación de los contratos con consumidores en mercados tradicionales la regulación de las transacciones consumidores en mercados digitales presenta elementos distintivos desde el punto de vista de la información precontractual que el consumidor debe disponer,[1] de la formación del contrato,[2] de la naturaleza del objeto del contrato – digital o no,[3] del control del contenido del contrato[4] y de los remedios disponibles para el consumidor en caso de incumplimiento contractual.[5]

Aunque formalmente distintos y regulatoriamente autónomos, las dos fases que configuran la contratación con consumidores en mercados digitales - la política de privacidad y la configuración contractual de la transacción digital - se encuentran íntimamente relacionados y el primero, en este caso la política de privacidad, tiene efectos o puede tenerlos sobre la configuración del segundo con efectos importantes para el bienestar del consumidor.[6] Es decir, los datos personales del consumidor son un elemento

---

[1] Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, *OJ L 149, 11.6.2005, p. 22–39 (https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32005L0029)* y la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011 , sobre los derechos de los consumidores, *OJ L 304, 22.11.2011, p. 64–88.*

[2] En derecho español, por ejemplo, los requisitos de formación contractual se encuentran en el artículo 1261 del Código Civil.

[3] Directiva (UE) 2019/770, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales *OJ L 136, 22.5.2019, p. 1–27.*

[4] Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores, *L 095, 21 Abril de 1993, p. 0029 – 0034* (en adelante Directiva 93/13 sobre cláusulas abusivas).

[5]Directiva 2019/771 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes, por la que se modifican el Reglamento (CE) n.° 2017/2394 y la Directiva 2009/22/CE y se deroga la Directiva 1999/44/CE (Texto pertinente a efectos del EEE.) PE/27/2019/REV/1, *OJ L 136, 22.5.2019, p. 28–50 (https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32019L0771).* Véase también la Directiva 2019/2161 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión. OJ L 328, 18.12.2019, p. 7–28 (llamada Directiva Omnibus) (https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019L2161).

[6] ZUIDERVEEN BORGESIUS, F. POORT, J., «Online Price Discrimination and EU Data Privacy Law», *J. Consum Policy* 40:347-366 (2017).

muy valioso para una eventual configuración de la transacción presente pero también para el diseño y contenido de eventuales transacciones futuras con el consumidor.

La decisión y configuración de las políticas de privacidad y por lo tanto la decisión sobre qué datos compartir y qué tratamientos de dichos datos se considerarán aceptables y por lo tanto se van a permitir son un elemento anterior y generalmente presente a cualquier actividad digital. Como se explicará en los siguientes apartados, la naturaleza de los datos personales hace que los individuos no estén bien posicionados para poder realizar una correcta evaluación del contenido de las políticas de privacidad y de sus efectos sobre su bienestar tanto en el presente como en el futuro.

III. EL MODELO AUTODETERMINISTA – AUNQUE NO CONTRACTUAL – DEL RÉGIMEN DE PROTECCIÓN DE DATOS EN EUROPA

En el momento de visitar una página web, bajar una aplicación online o participar en un mercado digital de doble cara la primera decisión que debe afrontar el eventual consumidor es aceptar rechazar o configurar de forma personalizada la política de privacidad. La política de privacidad se refiere a los términos en los que, por ejemplo, la plataforma el sitio web o el mercado de doble cara, podrá acceder y eventualmente tratar los datos personales del individuo-consumidor que forman parte de su privacidad.

Las políticas de privacidad tienen una estructura muy parecida a los contratos con condiciones generales de la contratación: el predisponente solicita el acceso y eventual tratamiento de determinados datos personales del interesado a cambio que este pueda acceder a la información proporcionada en la página web, a bajarse la plataforma digital en su teléfono móvil o tableta, o eventualmente participar en el mercado de doble cara como consumidor o eventualmente como vendedor. El interesado - consumidor - tiene la posibilidad de aceptar rechazar o configurar el acceso y tratamiento de sus datos personales a cambio de acceder a información servicio o participar en un determinado mercado de doble cara.

Desde el punto de vista estructural la decisión sobre el acceso y el procesamiento de los datos es muy parecida a la estructura de un contrato: el acceso y eventual tratamiento de los datos personales del interesado - consumidor – es equivalente a la contraprestación al acceso a un determinado servicio digital o a la participación de un determinado mercado de doble cara.[7] Así, el consentimiento o ámbito de consentimiento del interesado - consumidor - constituye la base de acceso y eventual tratamiento de sus datos personales.

[7] Independientemente de su caracterización doctrinal, los tribunales a menudo han considerado las políticas de privacidad como contratos. Véase BEN-SHAHAR, O. y STREHILEVITZ, L.J.,

«Contracting over Privacy: Introduction», *The Journal of Legal Studies* 45(S2) (2016) refiriéndose a la práctica jurisprudencial en los tribunales federales norteamericanos

A pesar de la similitud estructural entre los contratos y las políticas de privacidad,[8] el régimen de Protección de Datos Europeo no se configura, en un principio, como un contrato entre un sujeto eventualmente consumidor y un profesional en base a entender la naturaleza del derecho fundamental de la privacidad del sujeto consumidor y por lo tanto considerar que los datos personales no pueden constituir una contraprestación necesaria para el acceso a páginas plataformas o mercados de doble cara digitales.[9] El derecho a la privacidad concretamente el derecho a mantener privados datos personales es un derecho fundamental previsto en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos.[10] Aunque la estructura de las políticas de privacidad se parezcan significativamente a la estructura de un contrato la diferencia fundamental se encuentra en que al ser los datos personales un derecho fundamental del individuo consumidor estos no pueden considerarse una contraprestación necesaria para el acceso a la página web plataforma o mercado digital de doble cara. Por lo tanto, el rechazo o falta de consentimiento del individuo consumidor al acceso y eventual procesamiento de sus datos personales no podría constituir una base para denegar su acceso a la página web plataforma o mercado digital de doble cara.[11]

"*To date, among 51 cases in which courts addressed this issue, only in five cases did courts decide that privacy notices are not contracts*. All the remaining cases treated privacy otives as contracts."

[8] Véase id. considerando que la caracterización de las políticas de privacidad como contratos tiene dos efectos positivos importantes por un lado, limitar la responsabilidad de los profesionales empresarios por la gestión de los datos de los consumidores y por otro, asegurar a los consumidores que algún tratamiento de sus datos que se realizarían sin su consentimiento, no se llevarán a cabo.

[9] NORTON, Th. B., «The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model», 27 *Fordham Intell. Prop. Media & Ent. L.J.* 181 (2016). Disponible en https://ir.lawnet.fordham.edu/iplj/vol27/iss1/5. La determinación de la naturaleza contractual de las políticas de privacidad está en estos momentos pendiente ante el Tribunal de Justícia Europeo en el caso C 446/21 Schrems v. Facebook ireland Ltd. presentado por el Tribunal Supremo de Austria el pasado 20 de julio de 2021.

[10] Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) (https://www.europarl.europa.eu/charter/pdf/text_es.pdf) establece:

Artículo 8 - Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[11] Desde el punto de vista normativo no es posible condicionar el acceso o ámbito de acceso del interesado a la página o el mercado digital como respuesta al rechazo al acceso a sus datos personales. Si el consentimiento o falta de consentimiento tuviera consecuencias en el estatus del interesado en el ámbito digital el consentimiento prestado no se podría considerar como libre sino condicionado a una contraprestación. Merece la pena señalar que dicho condicionamente es técnicamente posible – a día de hoy desconocemos su uso. Véase BEN-SHAHAR, O. y SCHNEIDER, C., «The Failure of Mandated Disclosure», 159 *University of Pennsylvania Law Review* 647 (2011) y FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J.

Merece la pena señalar, no obstante, que des del punto de vista formal – aunque no sustantivo - la estructura de las políticas de privacidad es significativamente parecida a la estructura de un contrato. En gran parte esta similitud deriva de la importancia y rol del consentimiento del individuo consumidor cómo elemento esencial para permitir el acceso y eventual procesamiento de sus datos personales.[12]

La evidencia empírica sugiere que los interesados - entre los cuales se encuentran los consumidores - en su gran mayoría consienten al acceso y tratamiento de sus datos personales de acuerdo con lo previsto en las políticas de privacidad de las páginas web plataformas y mercados de doble cara digitales que visitan y que eventualmente terminan por aceptar en su totalidad.[13] El modelo europeo de Protección de Datos se basa en el consentimiento del individuo que, sin ser una contraprestación contractual, constituye el elemento imprescindible, necesario y suficiente para permitir el acceso y tratamiento a sus datos personales.[14] Los problemas y limitaciones que presenta el consentimiento como elemento fundamental del modelo de Protección de Datos en Europa se presentará en la sección siguiente.[15]

La configuración normativa de la Protección de Datos en Europa se estructura alrededor de un modelo de propiedad y control de los datos personales por parte de los interesados y de su gestión en base a su autonomía privada. El régimen de Protección de Datos en Europa se basa en (a) entender que la privacidad es un derecho fundamental,[16] (b) asegurar la libre circulación de dichos datos en el mercado europeo y finalmente en (c)

Eisler (eds), *DATA-DRIVEN PERSONALISATION IN MARKETS, POLITICS AND LAW*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

[12] STRANDBURG, K. J., «Free Fall: The Online Market's Consumer Preference Disconnect», 2013 *U. Chicago Legal F.* 95 (2013) considerando que los datos personales se podrían considerar una contraprestación contractual si proporcionaran información sobre las preferencias del interesado, de la misma forma que los precios proporcionan esta información sobre los bienes y servicios que los consumidores compran.

[13] ACQUISTI, A. y GROSSKLAGS, J., «What can behavioral economics teach us about privacy?», en A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES*, Boca Raton: Auerbach Publications, p. 363-377 (2007).

[14] WARNER, R. y SLOAN, R., «Beyond Notice and Choice: Privacy, Norms, and Consent», *J. High Tech. L.* (2013). Disponible en https://scholarship.kentlaw.iit.edu/fac_schol/568

[15] FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *DATA-DRIVEN PERSONALISATION IN MARKETS, POLITICS AND LAW*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

[16] La configuración de la protección de datos como derecho fundamental se encuentra en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), el artículo 8 del Convenio para la Protección De Los Derechos Humanos y de las Libertades Fundamentales (1950) y el Convenio 108 del Consejo de Europa de 28 de enero de 1981 (ahora comúnmente conocido como Convenio 108+) (CETS No. 108), de 28 de Enero de 1981. España ha ratificado en 2021 el protocolo Protocolo Adicional que moderniza el Convenio. Véase MARTÍNEZ LÓPEZ-SÁEZ, M., «La ratificación española del Convenio 108+: consideraciones jurídicas básicas del nuevo marco Paneuropeo de protección de datos», *Revista General de Derecho Europeo*, núm 54 (2021).

armonizar el régimen jurídico de la Protección de Datos para asegurar un nivel de protección uniforme donde circulen libremente dichos datos. Los instrumentos jurídicos que forman el régimen de Protección de Datos en Europa se estructuran esencialmente a través del Reglamento General de Protección de Datos adoptado en 2016[17] y a través de la Directiva relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas, que se presentarán a continuación.[18] Estos textos constituyen la regulación fundamental relativa a la definición de datos personales, a los distintos mecanismos de acceso y obtención de dichos datos y a la legitimidad de su uso.

3.1. El concepto de datos personales

El Reglamento de Protección de Datos se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.[19] La definición de datos personales se encuentra en el artículo 4.1 del mismo reglamento[20] y se articula a través de cuatro elementos (a) toda información, (b) relativa a (sobre), (c) una persona física, (d) identificada o identificable.[21]

---

[17] Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), OJ L 119, 4.5.2016, p. 1–88 (https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679) (en adelante, Reglamento de Protección de Datos).

[18] Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, OJ L 201, 31.7.2002, p. 37–47(https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32002L0058&from=EN) (en adelante, Directiva sobre la privacidad y las comunicaciones electrónicas)

[19] Artículo 2.1 del Reglamento de Protección de Datos.

[20] Artículo 4.1 del Reglamento de Protección de Datos establece que:

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

[21] El Considerando [14] del Reglamento de Protección de Datos deja fuera del ámbito de aplicación del Reglamento los datos relativos a personas jurídicas. El TJUE parece haber adoptado una interpretación ámplia de lo que constituyen datos personales. Véase la sentencia del TJUE C 582/14 Patrick Breyer v Bundesrepublik Deutschland de 19 de octubre de 2016 en la que el Tribunal entendió que "*una dirección de protocolo de Internet dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal*."

La información de la persona física que se encuentra dentro del ámbito de aplicación del reglamento de Protección de Datos hace referencia a, por ejemplo, el nombre, lugar de residencia, lugar de trabajo, estatus económico y características personales culturales y sociales del individuo.[22] Los datos relativos a, por ejemplo, las características raciales del individuo, historial genético o médico se consideran datos sensibles y tienen un nivel de protección especial – y más elevado - dado que podrían afectar el ejercicio de derechos fundamentales del sujeto.[23]

La información sobre la persona física se consideran datos personales y por lo tanto se encuentran en el ámbito de aplicación material del Reglamento de Protección de datos cuando esta información identifique o permita, de forma directa o indirecta, la identificación de la persona física.[24]

---

[22] Por ejemplo, los datos contenidos en registros públicos relativos a una solicitud de permiso de residencia son datos personales (TJUE C 141/12 y C372/12 YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S, de 17 de julio de 2014 interpretando el artículo 12 (a) de la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos *OJ L 281, 23.11.1995, p. 31–50* - actualmente derogada por el Reglamento de Protección de Datos - y del artículo 8(2) de la Carta de Derechos Fundamentales de la Unión Europea. Igualmente, las respuestas a un examen profesional por parte de un aspirante y los comentarios proporcionados por un examinador profesional constituyen datos personales (TJUE C 434/16 Peter Nowalk v. Data Protection Commissioner de 20 de Dicembre de 2017 interpretando los artículos 12 (a) y (b) de la Directiva Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos *OJ L 281, 23.11.1995, p. 31–50* - actualmente derogada por el Reglamento de Protección de Datos).

[23] Considerando [51] del Reglamento de Protección de Datos. El tratamiento de los datos personales sensibles ha sido objeto de atención por parte del TJUE. En la sentencia TJUE C136/17 GC y otros v. Commission nationale de l'informatique et des libertés (CNIL) de 24 de septiembre de 2019, el tribunal europeo entendió que un motor de búsqueda debe comprobar la legalidad del tratamiento de datos personales sensibles solamente con posterioridad a recibir, por ejemplo, una petición de eliminación de dichos datos. Este caso aclaró algunos de los aspectos interpretables de la sentencia Google Spain, S.L., v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González C131/12 de 13 de mayo de 2014 que aunque era posible interrpetar que proporcionaba un nivel elevado de protección de datos personales, dejaba muchos aspectos pendientes de interpretación. Véase GLOBOCNIK, J., **«**The Right to Be Forgotten Is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)**»,** 69 GRUR Int. 4 (2020). El Reglamento no hace mención ni resuelve el problema que se plantea cuando el tratamiento de los datos personales puede dar lugar a inferir y eventualmente conocer datos considerados sensibles bajo el Reglamento de Protección de Datos. Véase FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

[24] Considerando [26] del Reglamento de Protección de Datos establece que se considerará identificable aquella información que derive directamente del sujeto, pero también aquella información que, aunque seudonimizada, permita identificar al sujeto cuando se combine con información adicional.

3.2. Mecanismos de acceso y obtención de datos personales

El acceso a los datos personales de los individuos se lleva a cabo de forma muy diversa y a través de mecanismos muy heterogéneos. Las páginas web disponen de mecanismos para conocer el historial de la navegación del individuo – a través de cookies -, para identificar su lugar de conexión – a través de las direcciones IP -, para trazar los dispositivos – a través de las llamadas *device fingerprints* -, la obtención de información personal a través de las llamadas *pixel tags* – pixels identificadores que se cargan cuando un individuo visita una página web o abre un correo electrónico, o identificadores publicitarios – identificadores proporcionados por Google play para monetizar las aplicaciones de forma más efectiva.[25]

Todos estos mecanismos, utilizados individualmente o de forma combinada permiten obtener datos personales del interesado, pero también realizar un seguimiento continuo de su actividad digital que, junto al análisis de su comportamiento y actividad digital permiten obtener inferencias y predicciones que proporcionan una información tremendamente valiosa para conocer, predecir y eventualmente monetizar los servicios que se proporcionan a los individuos.

3.3. El tratamiento de los datos personales

El acceso a los datos personales de los interesados, como se ha explicado anteriormente, es de especial importancia tanto para las plataformas como para las empresas y para los gestores de los mercados digitales porque permiten conocer el perfil de los individuos que visitan sus páginas participan en sus mercados o en sus plataformas - por ejemplo, su edad, localización o sus intereses. El valor de estos datos personales, sin embargo, va mucho más allá del dibujo de las características, preferencias y gustos presentes de los usuarios de determinadas páginas mercados o plataformas digitales.

El *machine learning* y la inteligencia artificial permiten, a través del tratamiento de los datos personales obtenidos a través de la actividad online de los interesados, dibujar con remarcable exactitud un perfil del individuo, de sus características personales educativas sociales y económicas, de sus gustos preferencias y decisiones que toma en los mercados digitales, correlacionarlo con su contexto social profesional y familiar e inferir sus gustos y decisiones futuras.

---

[25] Véase COFONE, I., «Beyond Data Ownership», 43 *Cardozo Law Review* (2021, en prensa) y FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

El tratamiento de los datos personales de los individuos está permitido en el reglamento de Protección de Datos. El Reglamento de Protección de Datos establece que "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*" constituirá el tratamiento de datos.[26] El tratamiento de datos personales debe llevarse a cabo de forma (1) lícita, (2) leal y (3) transparente[27] y a su vez deberá estar limitado al fin (1) determinado, (2) explícito y (3) legitimo[28] al que haya prestado consentimiento el individuo.

A través del *machine learning* y la inteligencia artificial, los datos personales de los individuos pueden agregarse y obtener así información muy exacta de su perfil como consumidor, elector, vecino y ciudadano en general. Este conocimiento tiene un valor económico muy relevante tanto para los vendedores como para los gestores del mercado – y para los poderes públicos, siempre interesados en conocer las preferencias y variables relevantes para sus ciudadanos y eventualmente votantes.[29] Conocer las preferencias, gustos y decisiones de los individuos a través de su actividad digital permite personalizar la información, las sugerencias de compra, la visualización de los productos en cada página, y eventualmente los contratos que los consumidores digitales aceptan al realizar una transacción online. En definitiva, a través del *machine learning* y la inteligencia artificial el tratamiento de datos personales de los individuos permite personalizar la experiencia informativa, comercial, publicitaria y contractual del consumidor en mercados digitales.

La personalización de la experiencia del consumidor en mercados digitales - a través de publicidad personalizada, de la información precontractual ajustada a las características del consumidor y del contrato que regule los términos de la transacción, entre otros – no es en sí ni negativa ni positiva para el consumidor. Sin embargo, la asimetría informativa entre las partes contractuales en entornos digitales coloca, como se explicará más adelante, al consumidor en una posición de especial vulnerabilidad para asegurar un nivel de bienestar en las transacciones digitales como mínimo equivalente al que éste obtendría en transacciones tradicionales.

---

[26] Véase el artículo 4.2 del Reglamento de Protección de Datos.

[27] Véase el artículo 5.1 del Reglamento de Protección de Datos.

[28] Véase el artículo 5.2 del Reglamento de Protección de Datos.

[29] Las implicaciones de los datos personales para el ejercicio y respeto de los derechos fundamentales de los ciudadanos queda fuera del ámbito de este artículo.

3.4. Los derechos de los sujetos relativos al acceso y tratamiento de sus datos personales

Desde el punto de vista del acceso a los datos del individuo por parte de las organizaciones el Reglamento de Protección de Datos prevé distintos derechos. Por un lado, los individuos tienen derecho a ser informados de los datos personales a los cuales se accede y sobre el tratamiento que se les da.[30] Por otro lado, los individuos tienen derecho a conocer y acceder a los datos que las organizaciones tienen sobre ellos, a rectificarlos y eventualmente a suprimirlos si lo consideraran conveniente.[31]

En primer lugar, los individuos tienen derecho a ser informados de forma clara y comprensible de los datos a los que las distintas organizaciones páginas webs plataformas o mercados de doble cara acceden coma cómo los utilizan coma por cuánto tiempo y eventualmente si éstos serán compartidos con terceros.

A continuación, los individuos tienen derecho a acceder a los datos que las organizaciones disponen sobre ellos y a saber cómo se utilizan. Las organizaciones disponen de un mes para proporcionar dicha información.[32]

La gestión de los datos personales por parte de los individuos bajo el régimen previsto por el Reglamento de Protección de Datos incluye el derecho de rectificación y el derecho de eliminación de dichos datos, el llamado derecho al olvido. Por ejemplo, en aquellos casos en los cuales un individuo considera que los datos personales que una organización tiene sobre él son inexactos o incompletos, éste puede requerir a la organización que los rectifique. Por otro lado, los individuos pueden solicitar a las organizaciones que eliminen sus datos en los casos en los que el individuo entienda que estos ya no son necesarios o no persiguen el objetivo que tenían cuando éste consintió a su acceso. Es decir, el individuo puede, en cualquier momento revocar el consentimiento que eventualmente haya proporcionado al acceso y tratamiento de sus datos personales.

Los derechos de información, acceso, rectificación y eliminación de los datos del individuo son derechos que permiten, bajo el régimen jurídico previsto por el Reglamento, el control y gestión de dichos datos por parte del individuo.

Un segundo grupo de derechos tiene que ver con la utilización y tratamiento de dichos datos y el eventual acceso que puedan tener terceros a estos. En este sentido el Reglamento de Protección de Datos proporciona a los individuos el derecho a determinar si las organizaciones podrán tratar estos datos y agregarlos con datos de otros individuos

---

[30] Véase el artículo 5 del Reglamento de Protección de Datos

[31] Artículo 13.2(b) del Reglamento de Protección de Datos.

[32] Artículo 14.3 del Reglamento de Protección de Datos.

de forma que puedan obtener información resultante de los datos personales que los individuos han accedido a compartir. El tratamiento de los datos personales permite a las organizaciones obtener metadatos que proporcionan información sobre, por ejemplo, las características de los consumidores, de sus preferencias o de su capacidad económica. La decisión del interesado respecto al tratamiento de sus datos personales puede ser afirmativa consintiendo por lo tanto a dicho tratamiento, negativa - rechazándolo - o personalizada determinando el tratamiento al que el interesado accede. A su vez, los interesados también pueden decidir sobre la portabilidad de los datos de una organización a otra a través por ejemplo de una portabilidad contractual en a un contrato de telefonía o un contrato de un servicio a electrónico. Adicionalmente el Reglamento de Protección de Datos permite la utilización de la información obtenida a través del procesamiento de los datos del individuo para la personalización de las transacciones al perfil del interesado en cuestión.[33] Merece la pena señalar que si los términos de la transacción ofrecida al consumidor fueran completamente automatizados el Reglamento de Protección de Datos impone una obligación de información bajo la cual el interesado debe ser informado que la transacción es el resultado de un proceso totalmente automatizado.[34]

IV. LAS INHERENTES LIMITACIONES DEL MODELO AUTODETERMINISTA DE PROTECCIÓN DE DATOS

El armazón de la regulación de Protección de Datos en la Unión Europea se estructura alrededor del individuo – interesado en lenguaje del Reglamento. El interesado, la persona física - eventualmente un consumidor - los datos de la cual se accede, es el agente que ostenta el control sobre sus datos personales y los gestiona. Este control, esencialmente privado, se entiende posible en base a la información transparente al que el interesado tiene derecho relativa al acceso y tratamiento de sus datos personales y anterior a la prestación de consentimiento.

Así, el reglamento de Protección de Datos se configura a través de la transparencia de la información para el interesado y el control y gestión del interesado en el acceso y tratamiento de sus datos personales a través del consentimiento. En primer lugar, el Reglamento de Protección de Datos requiere que el interesado reciba información transparente relativa al acceso y tratamiento a sus datos. Por otro lado, la autonomía privada del individuo se materializa a través del consentimiento como instrumento esencial para que el interesado controle y gestione el acceso y tratamiento de sus datos personales,

[33] ZUIDERVEEN BORGESIUS, F. POORT, J., «Online Price Discrimination and EU Data Privacy Law», *J. Consum Policy* 40:347-366 (2017).

[34] Artículo 22 del Reglamento de Protección de Datos.

revoque el consentimiento eventualmente prestado para así modificar el ámbito de acceso y tratamiento a los datos personales o incluso lo elimine.[35]

Es un modelo esencialmente de derecho privado que considera los datos personales como cualquier otro bien objeto derechos reales, concretamente de derechos de propiedad, sobre el cual el individuo puede decidir lo que considere.[36]

Esta estructura, sin embargo, plantea dudas importantes respecto su efectividad. La naturaleza de los datos personales es muy distinta a la de los bienes muebles e inmuebles, la propiedad de los cuales se ha regulado tradicionalmente a través de derechos reales.[37] Por otro lado, la dimensión temporal y colectiva de los datos personales no permite que el inidividuo, en el momento de prestar consentimiento, pueda evaluar y valorar el contenido y efectos, tanto presentes como futuros, de dicho consentimiento y, finalmente, las limitaciones cognitivas y racionales de los individuos sugieren que este enfoque no es el más adecuado para la protección de datos, particularmente respecto los datos de los consumidores.

Las tres variables que definen las limitaciones inherentes del modelo de protección de datos europeo se desarrollarán a continuación.

4.1. *La naturaleza de los datos personales*

Los datos personales, concretamente los digitales, tienen una naturaleza etérea, no perceptible y difícilmente calculable. Esta naturaleza ni física ni concreta dificulta a las personas ser conscientes de los elementos, variables y contenido de los datos personales. Resulta muy difícil para los individuos conocer y valorar las variables personales que constituyen datos relevantes a los cuales las páginas plataformas o aplicaciones desean tener acceso y a su vez conocer y entender el tratamiento estadístico y matemático que se va a llevar a cabo con estos datos. Es difícil por lo tanto para los individuos configurar las políticas de privacidad con pleno conocimiento de los datos sobre su persona a los que

---

[35] Véase CALO, R., «Against Notice Skepticism in Privacy (and Elsewhere)», 87 *Notre Dame L. Rev.* 1027, 1047–59 (2011) defendiendo el modelo de protección de datos basado en el consentimiento del interesado.

[36] SOLOVE, D. J., «Privacy Self-Management and the Consent Dilemma», 126 *Harv. L. Rev.* 1880, 1882–83 (2012) y FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021). Para una visión crítica véase COFONE, I., «Beyond Data Ownership», 43 *Cardozo Law Review* (2021, en prensa).

[37] Véase VICTOR, J. M., «The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy», Note, 123 *Yale L. J.* 513, 515 (2013) argumentando que el llamado derecho al olvido y la portabilidad de los datos por parte del interesado en el Relgamento de Protección de datos son elementos inspirados en los derechos de propiedad sobre bienes muebles e inmuebles.

se acceden su tratamiento estadístico y matemático y los resultados que eventualmente se van a obtener de estos.

Las dificultades relativas al conocimiento y evaluación de los datos personales y de su relevancia para el bienestar presente y futuro del individuo hacen muy costoso para el individuo prestar un consentimiento informado. Es razonable, por lo tanto, que el individuo preste consentimiento minimizando el coste que le representa acceder a la página plataforma o bajarse la aplicación digital en cuestión. La naturaleza de los datos personales hace que invertir un mayor tiempo y esfuerzo en conocer y evaluar el impacto de la política de privacidad en el bienestar del individuo sea en la mayoría de los casos una pérdida de tiempo y por lo tanto en un coste que no sea racional asumir.

Por otro lado, la naturaleza abstracta y etérea de los datos personales dificulta también la consciencia y por lo tanto la reacción de los individuos en relación a la vulneración de su privacidad o del incumplimiento de la normativa de Protección de Datos. En muchos casos es difícil para los individuos conocer que sus datos personales han sido publicados, que su información bancaria ha sido accesible, aunque sea durante un breve periodo de tiempo o que sus nombres de usuario y contraseñas para acceder a distintas cuentas personales han sido publicadas. Pero incluso en los casos en los cuales los individuos conocen que es su privacidad ha sido vulnerada y que sus datos han sido publicados es difícil evaluar el daño que se sufre a causa de la vulneración de privacidad. Es decir, ¿cuál es el daño causado por la publicación del nombre de usuario y la contraseña de acceso a una red social de un individuo? ¿cuál es el daño causado por la publicación de las características personales sociales y económicas de un individuo anonimizadas? el individuo ha visto vulnerada su privacidad y el daño indudablemente existe. El problema se encuentra en su cuantificación.

Las dificultades relativas a la cuantificación de los daños resultantes de la vulneración de la privacidad de los individuos diluyen la estructura de incentivos del régimen de Protección de Datos: [38] si los individuos no son conscientes de la vulneración de su derecho y que éste eventualmente ha resultado en un daño es difícil que la víctima tenga incentivos para interponer una demanda de responsabilidad con el objeto de resarcirse de los daños que ha sufrido. A su vez anticipando la improbable acción judicial de la víctima las páginas web plataformas y aplicaciones digitales tienen pocos incentivos para tomar medidas efectivas que protejan los datos y la privacidad de sus usuarios.

No es posible, por lo tanto, alinear los incentivos de las partes eventualmente afectadas por la vulneración de la normativa de protección de datos y por lo tanto no es posible

[38] La regulación de las exernalidades negativaas que genera la vulneración de la la protección de los datos personales de los individuos son los posibles regularla desde el derecho público. Véase BEN-SHAHAR, Omri, «Data Pollution», *Journal of Legal Analysis*, Vol. 11, pp. 104–159 (2019).

obtener un resultado óptimo en relación a las medidas de cuidado por un lado y en relación a la interposición de acciones de responsabilidad para obtener compensación por los daños causados.

La imposible evaluación de las variables relevantes en las políticas de privacidad y de sus potenciales efectos y los resultados subóptimos en relación a los incentivos de las partes afectadas por incumplimiento de las políticas de privacidad limitan y cuestionan el rol fundamental del consentimiento en la protección de datos en Europa.

4.2. *La dimensión colectiva y dinámica de los datos personales*

Un segundo aspecto que dificulta un consentimiento informado y consciente sobre el acceso y tratamiento de los datos personales se encuentra en las dimensiones colectivas y dinámicas de su tratamiento.

El tratamiento de los datos personales se realiza a través de técnicas que utilizan el *machine learning* y la inteligencia artificial que permiten agregar cantidades ingentes de datos de múltiples individuos y así poder obtener correlaciones – tanto positivas y negativas- entre los datos de los individuos que permitan inferir información adicional sobre el individuo en cuestión así como anticipar probables decisiones futuras de los individuos para finalmente personalizar al máximo la experiencia informativa en el mercado, red social o buscador.

El tratamiento de los datos personales tiene una dimensión colectiva y una dimensión dinámica que dificultan – sino hacen imposible – que el interesado pueda valorar el contenido de las políticas de privacidad y los efectos que pudieran tener en su bienestar presente y futuro.

La dimensión colectiva del tratamiento de datos personales hace referencia a la necesaria agregación de datos personales con datos personales de otros sujetos y a las inferencias que las técnicas estadísticas y matemáticas permiten obtener acerca de las características de los individuos.[39] En el momento de prestar consentimiento el individuo desconoce cuáles serán los datos a los que se agregará su información personal, su tratamiento matemático y las inferencias que este tratamiento permitirá obtener. La dimensión colectiva de los datos personales, por lo tanto, obliga a un consentimiento ignorante.

Por otro lado, los datos personales tienen una dimensión estática y una dimensión dinámica. El consentimiento que se proporciona respecto al acceso a estos datos tiene

[39] FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

una naturaleza estática – e individual – mientras que el tratamiento de los datos personales tiene una naturaleza eminentemente dinámica -y colectiva. El contenido de este consentimiento y sus efectos es radicalmente distinto para el individuo.

La naturaleza del tratamiento de datos o de su portabilidad es dinámica. La naturaleza dinámica de estos derechos deriva del hecho que en el momento en el que el individuo presta consentimiento al tratamiento de sus datos personales - de forma total o parcial – consiente, o no, a un tratamiento o portabilidad que eventualmente tendrá lugar en el futuro – y que tendrá dimensiones que el individuo desconoce en el momento de consentir. De esta forma, en el momento de prestar consentimiento el consumidor desconoce el eventual uso e impacto que el tratamiento de estos datos pueda tener para su perfil y posición en transacciones en mercados digitales y concretamente para su bienestar en transacciones futuras en mercados digitales.

Las dimensiones colectivas de los datos personales y su naturaleza dinámica que tiene efectos sobre el bienestar futuro del individuo cuestionan de forma importante, el rol del consentimiento como elemento fundamental del régimen de protección de datos en Europa.

4.3. *La dicotomía entre consentimiento y control: asimetría contractual y limitaciones cognitivas de los interesados en el control y gestión de los datos personales*

Los individuos – eventualmente consumidores- no están bien posicionados para decidir sobre el acceso y tratamiento de sus datos. La paradoja de la privacidad[40] ilustra de forma muy gráfica este fenómeno que se explica en gran medida por las limitaciones cognitivas y racionales de los individuos. La paradoja de la privacidad muestra de forma experimental la contradicción existente entre la valoración de la privacidad que los individuos declaran y el comportamiento que muestran respecto su privacidad: mientras los individuos se declaran preocupados por su privacidad y le otorgan una valoración importante, sus decisiones son significativamente incoherentes con la valoración que confiesan dado que hacen poco, o esencialmente nada, para proteger sus datos personales.[41]

---

[40] BARTH, Susanne, D.T. de Jong, Menno, «The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A sytematic literature review», *Telematics and Informatics* 34(7) (2017).

[41] NORBERG, Patricia A., HORNE, D. R. y HORNE, D. A., (2007), «The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors», *Journal of Consumer Affairs*, 41 (1): 100–126 y

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences vs. Actual Behavior. In ACM EC'01, October 14–17, 2001.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences vs. Actual Behavior. In ACM EC'01, October 14–17, 2001.

Esta discrepancia se explica, en gran medida, por la posición asimétrica entre los individuos y las empresas que les solicitan consentimiento para acceder a sus datos personales[42] pero también por sus limitaciones cognitivas y racionales que no les permiten evaluar de forma efectiva el contenido y los efectos del consentimiento prestado respecto sus datos personales.

El consumidor se encuentra en una posición de vulnerabilidad y asimetría de información en el momento de aceptar, rechazar o configurar las políticas de privacidad que se le presenta. Los individuos en el momento de evaluar y tomar una decisión respecto la política de datos de la página web, mercado de doble cara o aplicación online, no conocen y tampoco pueden conocer el contenido y efectos de esta decisión.

En primer lugar y como se ha comentado anteriormente el consentimiento no parece el instrumento adecuado para gestionar los datos personales en base a la naturaleza dinámica – y colectiva - del tratamiento de los datos personales de los individuos. Entre los datos personales consiste en la agregación de los datos del interesado con datos de otros individuos para a través de técnicas estadísticas matemáticas del *machine learning* y la inteligencia artificial poder obtener metadatos que proporcionen información adicional sobre el interesado. No es posible por tanto que el interesado pueda conocer en el momento de prestar consentimiento cuáles son resultados probables de dicha agregación y por lo tanto cuál es la información que eventualmente se podrá obtener sobre él a través del tratamiento de sus datos en combinación con datos de otros individuos.[43]

Por otro lado, el elemento dinámico del tratamiento de los datos personales tiene que ver con la dicotomía temporal entre el momento de prestación del consentimiento al tratamiento de los datos personales y el momento en el cual se experimentan los efectos de dicho tratamiento. Así los efectos e impacto del tratamiento de los datos personales solo se pueden conocer y eventualmente evaluar en un momento futuro al de la prestación del consentimiento. El consentimiento del interesado a un eventual tratamiento de los

---

SPIEKERMANN, S., GROSSKLAGS, J. y BERENDT B., «E-privacy in 2nd Generation E-commerce: Privacy Prefereces vs. Actual Behavior», EC'01 *Proceedings of the 3rd ACM Conference on Electronic Commerce* (2001).

iekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-Privacy in 2nd Generation E-

Commerce: Privacy Preferences vs. Actual Behavior. In ACM EC'01, October 14–17, 2001.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. E-Privacy in 2nd Generation E-

Commerce: Privacy Preferences vs. Actual Behavior. In ACM EC'01, October 14–17, 2001

[42] ZUIDERVEEN BORGESIUS, F. POORT, J., «Online Price Discrimination and EU Data Privacy Law», *J. Consum Policy* 40:347-366 (2017).

[43] FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *DATA-DRIVEN PERSONALISATION IN MARKETS, POLITICS AND LAW*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

datos personales, por lo tanto, no se presta con toda la información relevante y necesaria dado que el impacto y efectos del tratamiento de los datos personales solo se materializarán en un futuro imposible de anticipar en el momento de prestar consentimiento.

Además, la decisión del individuo respecto sus datos en realidad no se toma respecto éstos sino respecto la posibilidad de acceder a una página web con información valiosa para el interesado, para instalar una aplicación que proporciona un servicio o finalmente para acceder a un mercado de doble cara. En otras palabras, la decisión del interesado se toma entre el acceso y eventual tratamiento de sus datos y el acceso al contenido de la página, la aplicación o el mercado de doble cara al que el interesado quiere participar.[44] Así, la evaluación y decisión sobre el acceso y tratamiento de los datos por parte del interesado no se toma únicamente respecto a estos, sino teniendo en cuenta, también, las preferencias más o menos estrictas del interesado respecto la página, aplicación o mercado al que quiere acceder que a su vez es quién presenta la política de privacidad al interesado.[45] Los dos elementos – acceso a los datos personales y tratamiento de éstos – se canalizan a través de un único consentimiento aunque son elementos sobre los cuales los individuos pueden tener preferencias distintas con elasticidades distintas.

En segundo lugar, los individuos – interesados en base el Reglamento de Protección de datos – presentan limitaciones cognitivas y racionales que no les permiten tomar decisiones racionales, en este caso en relación a las políticas de privacidad. Los interesados no están bien posicionados para que en caso que lo hicieran, leer, entender y evaluar complejas políticas de privacidad redactadas en muchos casos de forma difícil de entender[46] y eventualmente evaluar –en caso que fuera posible – sus efectos presentes y futuros para su bienestar en plataformas y mercados digitales.[47] Estas limitaciones, ampliamente estudiadas por la economía del comportamiento, cuestionan de forma

---

[44] La elasticidad de la decisión del interesado respecto al acceso a los datos personales puede ser diferente a la que éste tenga respecto al tratamiento de dichos datos personales. El Reglamento de Protección de Datos deja fuera esta dualidad.

[45] Véase GONZALEZ, E. y DE HERT, P., «Understanding The Legal Provisions That Allow Processing And Profiling Of Personal Data—An Analysis Of GDPR Provisions And Principles», 19 *ERA F.* 597, 600 (2019) considerando que el consentimiento del interesado es un instrumento válido cuando éste es el resultado de una decisión libre, genuina y no contaminada y cuestionando que el consentimiento respecto las políticas de privacidad tenga esta naturaleza.

[46] REIDENBERG, J. R., BHATIA, B., BREAUX, T. D., y NORTON, Th. B., «Ambiguity in Privacy Policies and the Impact of Regulation», 163 *Journal of Legal Studies* 45, p163–190 (2016) argumentando que además, las políticas de privacidad a menudo se modifican con posterioridad al consentimiento del interesado y por lo tanto, aunque formalmente notificado de la modificación, éste no conoce de forma efectiva el acceso y tratamiento de sus datos personales que se está llevando a cabo.

[47] BEN-SHAHAR, O. y STREHILEVITZ, L. J., «Contracting over Privacy: Introduction», *The Journal of Legal Studies* 45(S2) (2016).

importante la adopción de elementos tradicionales de la autonomía privada en la regulación de protección de datos en Europa.[48]

Una primera barrera al consentimiento efectivo de los interesados se encuentra en el hecho que los individuos no leen las condiciones generales de la contratación en un contrato y aún menos cuando éstas se encuentran en un contrato digital.[49] Incluso cuando los interesados - consumidores – hacen el esfuerzo de leer, la simplificación en la redacción de los contratos digitales no parecen tener ningún efecto en su comprensión y por lo tanto en el valor de dicho consentimiento.[50] La falta de lectura es el resultado de variables muy heterogéneas – falta de interés, tiempo, voluntad de realizar el esfuerzo – pero también de la cantidad de la información que se proporciona a los interesados. Los interesados están expuestos a una cantidad de información –excesiva - que no les permite distinguir entre lo relevante y lo irrelevante, entre lo deseable y lo inaceptable según sus preferencias.[51]

Esta falta de lectura se explica, como mínimo parcialmente, por las distintas limitaciones cognitivas y racionales que experimentan los individuos a la hora de tomar decisiones.[52] Estas limitaciones, inherentes a la condición humana, son de especial importancia en un contexto contractual, especialmente en relación a la contratación con consumidores. La contratación con consumidores es particularmente asimétrica. Los contratos están diseñados y redactados por los predisponentes profesionales y los consumidores, adherentes al contrato se encuentran en una posición particularmente vulnerable en base a la asimetría de información y de posición y capacidad de negociación y la posible utilización de las limitaciones cognitivas y racionales del consumidor adherente en el diseño contractual en beneficio del empresario profesional. Dos ejemplos de dichas

---

[48] SOLOVE, D.J., «Privacy Self-Management and the Consent Dilemma», 126 *Harv. L. Rev.* 1880, 1882–83 (2012).

[49] BAKOS, Y., MAROTTA-WURGLER F. y TROSSEN, D.R., «Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts», 43 *The Journal of Legal Studies* 1 (2014) y ACQUISTI, A. y GROSSKLAGS, J., «What can behavioral economics teach us about privacy?», en A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES*, Boca Raton: Auerbach Publications, p. 363-377 (2007).

[50] BEN-SHAHAR, O. y CHILTON, A. «Simplification of Privacy Disclosures: An Experimental Test», 45 *J. Legal Stud*. 41, 44 (2016).

[51] COFONE, I. y ROBERTSON, A. Z. «Consumer Privacy in a Behavioral World», 69 *Hastings L.J.* 1471, 1475, 1489–1490 (2018).

[52] WAGNER, G. y EIDENMÜLLER, H., «Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions», *The University of Chicago Law Review,* 86:581, 592-595 (2019).

limitaciones cognitivas y racionales son el descuento hiperbólico y el efecto marco que son especialmente relevantes a la hora de tomar decisiones contractuales.[53]

El descuento hiperbólico se refiere a la tendencia de los individuos a escoger alternativas que tienen un resultado – o pago – inmediato frente alternativas que quizás con un valor esperado mayor, se recibirían en el futuro. A la hora de valorar las alternativas, los individuos atribuyen un valor menor – descontado – a aquellas que eventualmente se realizará en el futuro. Este efecto es especialmente importante respecto las políticas de privacidad dado que el acceso a la página, aplicación o mercado de doble cara es inmediato mientras que sus efectos e impacto sobre el bienestar del interesado tendrá lugar eventualmente en el futuro. Así, la tendencia de los individuos será prestar consentimiento de forma inmediata las políticas de privacidad infravalorando los efectos que éstas tendrían en su bienestar futuro.

El efecto marco se refiere a la distinta respuesta que damos los individuos a decisiones que se plantean de una forma positiva o una forma negativa.[54] Es decir, cuando las decisiones se presentar en un marco positivo los individuos tendemos estar más dispuestos a aceptarlas. Cuando las alternativas se presentan desde un punto de vista negativo – enfatizando posibles pérdidas, por ejemplo – los individuos tenemos a no aceptarlas con tanta frecuencia. La información sobre los efectos de los datos personales para el futuro bienestar del individuo, su eventual pérdida de bienestar y el posible diseño de un perfil –como consumidor, por ejemplo – generalmente no se presentan a los interesados en forma de posibles pérdidas sino como elementos estáticos y eventualmente inocuos para el bienestar del individuo. En este contexto, la disposición a aceptar las políticas de privacidad por parte del interesado es mayor.

En este contexto no es posible para los interesados evaluar la información y los riesgos que presentan las políticas de privacidad para su bienestar. Esta evaluación es además virtualmente imposible cuando los datos personales del interesado se han agregado a otros datos y con éstos ha sido posible, en base a la inteligencia artificial y el *machine learning*, obtener inferencias sobre sus preferencias y decisiones y así dibujar un perfil del interesado con un elevado valor para mercados digitales y particularmente para los vendedores que participan en ellos.[55]

---

[53] ACQUISTI, A., BRANDIMARTE, L., y LOEWENSTEIN, G., «Privacy and Human Behavior in the Age of Information», 347 *Science* 6221, pp. 509-514 (2015) y ADJERID, I. y PE'ER, E. y ACQUISTI, A., «Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making», Carnegie Mellon University, Journal contribution (2018).

[54] KAHNEMAN; T., «The Framing of Decisions and the Psychology of Choice». *Science*. vol. 211, 30, p. 453 (1981).

[55] FINCK, M., «The Limits of the GDPR in the Personalisation Context», en U. Kohl, J. Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge: Cambridge University Press, *Max Planck Institute for Innovation & Competition Research Paper No.* 21-11 (2021).

Las limitaciones cognitivas y racionales de los individuos hacen que los individuos sean particularmente susceptibles a las percepciones de control o de falta de control sobre sus datos personales. Se puede dar en este caso, otra paradoja importante entre percepción de control y vulnerabilidad. Cuanto mayor es la percepción de control sobre los datos personales, mayor es la disposición a compartirlos. Sin embargo, cuanto mayor es la cantidad de datos personales que se comparte, mayor es la vulnerabilidad del individuo respecto los efectos de éstos para su bienestar futuro.[56]

¿Es necesariamente un problema que los individuos no dediquen esfuerzo, parte de su tiempo, esfuerzo y atención a leer políticas de privacidad y modular su consentimiento respecto éstas? Desde el punto de vista de la dimensión estática de los datos personales probablemente no sea un problema. Des del punto de vista de la dimensión dinámica de éstos, puede llegar a serlo.

Desde el punto de vista de la dimensión estática de los datos personales la falta de conocimiento a la hora de prestar consentimiento al acceso de los datos personales no es necesariamente problemática e incluso podría considerarse que es racional. Leer las políticas de privacidad lleva tiempo atención esfuerzo y requiere una formación y unos conocimientos que a menudo los individuos no tienen. No parece razonable asumir que todos los individuos puedan y deban dedicar un tiempo y un esfuerzo que podría resultar fructífero – o no – a leer, analizar, evaluar, entender y modular según sus preferencias Las políticas de privacidad que se le presentan en su actividad digital. Parece aún menos razonable presumir que todos los individuos en caso de que dedicaran este tiempo y esfuerzo se encontrarían en condiciones de entender y evaluar el contenido de las políticas de privacidad - tanto en relación al acceso a los datos personales como en relación a su tratamiento - de acuerdo con sus preferencias. El coste del esfuerzo, en muchos casos, será mayor que el beneficio en términos de mayor privacidad que perciba el individuo en cuestión. Por lo tanto, desde este punto de vista, parece razonable que los individuos no estén dispuestos a dedicar el tiempo y el esfuerzo a leer e informarse y evaluar políticas de privacidad que en un principio cumplen con lo previsto en el reglamento de Protección de Datos y en la normativa aplicable.

El análisis coste beneficio de los individuos en relación a las políticas de privacidad es significativamente distinto en relación a la dimensión dinámica – y colectiva - de los datos

[56] Este fenómeno es el llamado la paradoja de control que resulta en una mayor vulnerabilidad por parte de individuos que consideran que tienen gran control sobre sus datos. La percepción de control sobre los datos personales y sobre el consentimiento sobre su acceso y eventualmente sobre su tratamiento condiciona la futura mayor o menor vulnerabilidad del sujeto en su participación en mercados digitales. Véase BRANDIMARTE, L., ACQUISTI, A., y LOEWENSTEIN, G., «Misplaced Confidences: Privacy and the Control Paradox», *Social Psychological and Personality Science* (4:3), pp. 340-347 (2013).

personales. La sofisticación de las técnicas de tratamiento de datos personales hace que los costes de evaluación de los elementos dinámicos de los datos personales sean imposibles – infinitos - para el individuo. El tratamiento de datos es un fenómeno muy sofisticado técnicamente que conlleva la utilización de técnicas de *machine learning* y de inteligencia artificial que permiten la agregación de datos – con otros datos de terceros relacionados o no con el individuo y obtenido a través del consentimiento o a través de su compra en mercados de datos[57] - y la obtención de información muy valiosa sobre preferencias, perfiles e inferencias de comportamiento de los individuos – consumidores - de gran valor para las empresas.[58]

La complejidad del proceso de tratamiento de datos personales hace virtualmente imposible que el consentimiento del interesado sea fruto de un análisis racional e informado sobre su mecánica y efectos. La técnica estadística y computacional inherente al tratamiento de datos personales, la agregación de los datos personales y la utilización de los resultados para sugerir, anticipar y personalizar transacciones futuras presentan un nivel de complejidad imposible para el intelecto humano. Esta imposibilidad cuestiona la eficacia del consentimiento como instrumento de control para la dimensión dinámica de los datos personales desde al menos tres perspectivas. En primer lugar, para un individuo es racional no dedicar tiempo y esfuerzo a comprender y evaluar un fenómeno que se le anticipa virtualmente imposible. En segundo lugar, los individuos no pueden llevar a cabo la evaluación del tratamiento de los datos personales dado que dicho tratamiento combina los datos personales del individuo con datos e información de tercero que el individuo desconoce. Finalmente, el tratamiento de los datos personales proporciona una información que genera una externalidad en contratos futuros[59] que el individuo en el momento de evaluar la política de privacidad desconoce y que por lo tanto le es imposible evaluar.

El modelo de propiedad y control de los datos personales en base a la autonomía privada de los interesados con el consentimiento como elemento central del modelo presenta limitaciones importantes. El consentimiento no parece ser el instrumento adecuado para proteger la privacidad de los individuos y en particular la de los consumidores.

La protección de datos y por lo tanto de la privacidad de los individuos en su actividad digital – y concretamente la de los consumidores en su participación en mercados digitales

[57] SPIEKERMANN et al., S. «The Challenges of Personal Data Markets and Privacy», 25 *Electronic Markets* 161, 166–67 (2015).

[58] Y mucho más complejo que el análisis del acceso de los datos personales.

[59] BEN-SHAHAR, O. y STREHILEVITZ, L. J., «Contracting over Privacy: Introduction», *The Journal of Legal Studies* 45(S2) (2016).

– hace necesario contar, además, con alguna forma de control ex post por parte de los poderes públicos que combinada con el consentimiento ex ante pueda generar los incentivos adecuados para las partes.

V. ¿UN MODELO DE PROTECCIÓN DE DATOS EMINENTEMENTE PRIVADO O UN MODELO EFECTIVO?

Como se ha explicado anteriormente el modelo auto determinista de Protección de Datos en Europa presenta unas limitaciones tanto desde la perspectiva de la naturaleza de los datos, como de la complejidad y dimensiones que genera su tratamiento como de las limitaciones cognitivas y racionales de los individuos. Estas limitaciones no son ni nuevas ni exclusivas del modelo de Protección de Datos.[60] El estudio de la importancia de las limitaciones cognitivas y racionales de los individuos en contrato en la contratación con consumidores, por ejemplo, no son nuevos.[61] El estudio de la importancia del *machine learning* la inteligencia artificial en el tratamiento de cantidades masivas de datos – el big data - tampoco es un fenómeno nuevo. Por lo tanto, las limitaciones de los individuos a la hora de conocer comprender y gestionar políticas de privacidad en un formato muy parecido a los contratos y con un contenido no necesariamente asumible para un lego en la materia, son fácilmente previsibles.

El modelo europeo de Protección de Datos centrado en una visión de propiedad, control y autonomía privada eminentemente de derecho privado, aunque bien intencionado no parece responder de forma efectiva a la Protección de Datos y por lo tanto a la privacidad de los individuos que tiene encomendada.

Parece razonable plantearse sí en base a la complejidad matemática y jurídica de la regulación de Protección de Datos y por lo tanto de asegurar la privacidad de los individuos de acuerdo con sus preferencias no sería necesario, o incluso recomendable, adoptar normas de derecho público que regularán de forma general y anterior a las políticas de privacidad los datos a los que se puede acceder y en qué condiciones se pueden tratar, así como las consecuencias jurídicas de su incumplimiento. Las limitaciones inherentes del modelo privado de protección de datos en Europa hacen necesario incorporar normas que regulen de forma general el contenido de las políticas de privacidad que se entenderá compatible con garantizar la privacidad de los individuos. Por otro lado, el derecho privado se muestra inadecuado para poder gestionar las dimensiones colectivas de los datos, las

[60] WAGNER, G. y EIDENMÜLLER, H., «Down by Algorithms? Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions», *The University of Chicago Law Review,* 86:581, 592-595 (2019).

[61] Véase, por ejemplo, FAURE, M. G. y LUTH, H. A., «Behavioral Economics in unfair Contract terms», Journal of Consumer Policy, 34, pp 337-358 (2011).

inferencias que se pueden obtener en base a la agregación masiva de datos de distintos individuos, así como su dimensión dinámica. como se ha explicado anteriormente los datos tienen una dimensión estática pero también dinámica. Esta última hace imposible para los individuos poder evaluar, en el momento de prestar consentimiento o configurar la política de privacidad, los efectos e impacto del tratamiento que sus datos para su bienestar futuro. Finalmente, las acciones individuales por incumplimiento de las normas relativas a la Protección de Datos y por lo tanto los incumplimientos por vulneración de la privacidad de los individuos no son efectivas: en primer lugar, por la falta de incentivos individuales en interponer una acción para reclamar los daños eventualmente generados por el incumplimiento de la Protección de Datos personales y en segundo lugar, por la dificultad de la evaluación del daño individual generado por el incumplimiento de la protección de los datos personales del individuo. El modelo privado por lo tanto tampoco parece generar los incentivos adecuados para asegurar el cumplimiento del régimen de Protección de Datos.[62]

Por lo tanto, las limitaciones inherentes al modelo de régimen jurídico eminentemente privado de protección de datos en Europa requieren la adopción de normas de derecho público relativas al contenido de las políticas de privacidad – a los datos a los que será posible acceder -, al tratamiento que se podrá dar a los datos y finalmente a las consecuencias del incumplimiento del régimen jurídico de Protección de Datos.

El modelo europeo se basa en unas premisas que la práctica cuestiona de forma importante: en primer lugar, proporcionar información a los individuos no significa que estos conozcan y entiendan el contenido de dicha información. En segundo lugar, prestar consentimiento a políticas de privacidad no es equivalente a tener control sobre la gestión de los datos personales. La evidencia empírica disponible relativa a la eficacia – significativamente limitada - del modelo autodeterminista de protección de datos en Europa urge un replanteamiento - o como mínimo una actualización – del régimen jurídico.

Si el modelo europeo de Protección de Datos y de privacidad quieres ser eficaz, no parece posible dejar la protección y gestión de los datos personales solamente en manos de los individuos sin ningún filtro ex ante y supervisión ex post de naturaleza pública.

VI. CONCLUSIÓN

El modelo europeo de protección de datos, aunque bien intencionado, se está mostrando poco eficaz para proteger los datos y por tanto la privacidad de los individuos en su actividad digital.

[62] BEN-SHAHAR, Omri, «Data Pollution», *Journal of Legal Analysis*, Vol. 11, pp. 104–159 (2019).

Tanto la naturaleza de los datos personales como sus dimensiones colectivas y dinámicas como las limitaciones cognitivas y racionales de los individuos cuestionan el rol del consentimiento como elemento fundamental del sistema de protección de datos en entornos digitales.

El reglamento de protección de datos en Europa es relativamente joven pero la evidencia de su eficacia más que limitada en relación con la protección de la privacidad de individuos – y particularmente de consumidores - en su actividad digital y la rápida evolución de las técnicas de *machine learning* y de inteligencia artificial sugieren que el consentimiento del individuo no es suficiente para controlar y gestionar los datos personales de acuerdo con las preferencias de los individuos relativas a privacidad.

La naturaleza de los datos, sus dimensiones incontrolables por los individuos y la naturaleza de los individuos requiere la adopción de normas de derecho público que regulen, de forma previa y general los datos personales a los que se podrá acceder, los tratamientos que se considerarán aceptables y finalmente, el uso que se podrá dar a los resultados obtenidos.

Los retos que plantean el acceso y uso de los datos personales en la actividad digital y la vulnerabilidad en la que coloca a los individuos para decidir y reaccionar ante vulneraciones de su privacidad requieren una mejora del modelo.

No hacer nada no será para proteger el control y gestión privada de la privacidad de los individuos sino para transferir una responsabilidad que quizás, des del legislador comunitario, no se quiere asumir.

LA HIPOCRESÍA DE LA PROTECCIÓN DEL CONSUMIDOR EN LA ERA DE LA PUBLICIDAD CONDUCTUAL

Por

SÉBASTIEN FASSIAUX
Investigador predoctoral
Universitat Pompeu Fabra [1]

sebastien.fassiaux@upf.edu

Revista General de Derecho de los Sectores Regulados 8 (2021)

RESUMEN: La publicidad digital ha desempeñado un papel fundamental en el desarrollo de Internet tal y como lo conocemos. Las empresas han podido ofrecer nuevos productos y servicios en línea a los consumidores de forma gratuita, a cambio de sus datos personales que utilizan con fines de marketing. La industria de la tecnología publicitaria optó claramente por evolucionar hacia la publicidad basada en el comportamiento, recopilando grandes cantidades de datos personales para perfilar con precisión a los consumidores y ofrecer anuncios personalizados. Sin embargo, el desarrollo de la publicidad conductual creó importantes desafíos para los consumidores, especialmente en términos de privacidad y autonomía. Este artículo sostiene que el enfoque normativo tradicional sobre el consentimiento, la transparencia y el control ha sido hasta ahora ineficaz para proteger a los consumidores. La complejidad y la debilidad de la aplicación contribuyen además a la ineficacia de los derechos existentes, aunque los recientes avances positivos mitigan estos resultados. En este contexto, los consumidores parecen incapaces de protegerse contra las infracciones de las leyes de protección de datos. Este artículo sostiene que estos fallos del mercado justifican una mayor intervención reguladora, ya que, de lo contrario, la industria de la tecnología publicitaria seguirá quedando retratada y actuando como sus propios reguladores.

PALABRAS CLAVE: Publicidad conductual; inteligencia artificial; protección del consumidor; protección de datos; regulación.

SUMARIO: I. INTRODUCCIÓN. II. LA HISTORIA DE AMOR ENTRE LA PUBLICIDAD CONDUCTUAL Y LA INTELIGENCIA ARTIFICIAL. III. LA AUTONOMÍA DEL CONSUMIDOR ESTÁ EN PELIGRO EN LA ERA DE LA PUBLICIDAD CONDUCTUAL DIRIGIDA POR LA INTELIGENCIA ARTIFICIAL. IV. INEFICACIA DEL ENFOQUE NORMATIVO TRADICIONAL. 4.1. Consentimiento. 4.2. Transparencia. 4.3 Control. V. UNA APLICACIÓN COMPLEJA Y DÉBIL. 5.1. Aplicación privada. 5.2. Aplicación pública. VI. LA ILUSIÓN DE LOS REMEDIOS DE AUTOAYUDA. VII. NECESIDAD DE UNA MAYOR INTERVENCIÓN REGULADORA. VIII. CONCLUSIÓN. IX. BIBLIOGRAFÍA.

[1] Con el apoyo de la Secretaría de Universidades e Investigación del Departamento de Empresa y Conocimiento de la Generalitat de Cataluña y del Fondo Social Europeo.

ABSTRACT: Digital advertising has played a key role in the development of the internet as we know it. Firms have been able to offer new online products and services to consumers for free, in exchange for their personal data which they use for marketing purposes. The adtech industry clearly chose to evolve towards behavioral advertising, gathering large quantities of personal data to precisely profile consumers and deliver personalized ads. However, the development of behavioral advertising created important challenges for consumers, especially in terms of privacy and autonomy. This article argues that the traditional regulatory focus on consent, transparency and control has so far been ineffective at protecting consumers. Complex and weak enforcement further contributes to the ineffectiveness of existing rights, although recent positive developments mitigate these findings. In this context, consumers appear unable to protect themselves against infringements of data protection laws. This article argues that these market failures warrant further regulatory intervention, otherwise the adtech industry will continue to be portrayed and act as their own regulators.

KEYWORDS: Behavioral advertising; artificial intelligence; consumer protection; data protection; regulation.

I. INTRODUCCIÓN

La publicidad digital ha desempeñado un papel fundamental en el desarrollo de Internet tal y como lo conocemos. Las empresas han podido ofrecer nuevos productos y servicios en línea a los consumidores de forma gratuita, a cambio de sus datos personales que utilizan con fines de marketing. La industria de la tecnología publicitaria optó claramente por evolucionar hacia la publicidad basada en el comportamiento, recopilando grandes cantidades de datos personales para perfilar con precisión a los consumidores y dirigir los anuncios de forma personalizada. Este modelo es ahora omnipresente en el mundo digital y cada vez más en el analógico. La omnipresencia de este modelo se ve acentuada por el desarrollo de la inteligencia artificial (IA), que permite a las empresas dar más sentido a los grandes datos que recogen, no sólo con fines de marketing, sino también para construir potentes herramientas que sí requieren grandes cantidades de datos para aprender y hacer mejores predicciones. No es una coincidencia que Google y Facebook, algunos de los actores más destacados del sector de la tecnología publicitaria, estén también a la vanguardia de la innovación en IA (la sección 0explica la relación entre la publicidad basada en el comportamiento y la IA).

Sin embargo, el desarrollo de la publicidad basada en el comportamiento creó importantes desafíos para los consumidores, especialmente en términos de privacidad y autonomía, como se explica a continuación en la sección 0. Esto hace que la regulación de la protección de los consumidores y de los datos a nivel de la UE sea esencial. Sin embargo, este artículo sostiene que el enfoque normativo tradicional sobre el consentimiento, la transparencia y el control ha sido hasta ahora ineficaz para proteger a los consumidores (sección 0). La complejidad y la debilidad de su aplicación contribuyen además a la ineficacia de los derechos existentes, aunque los recientes avances positivos mitigan estos resultados (sección 0). En este contexto, el artículo sostiene que los consumidores son incapaces de protegerse contra las infracciones de las leyes de

protección de datos (sección 0). Por último, los fallos del mercado detallados en este artículo justifican una mayor intervención reguladora, ya que, de lo contrario, las grandes empresas tecnológicas, especialmente las activas en el sector de la tecnología publicitaria, seguirán retratándose y actuando como sus propios reguladores (sección 0).

II. LA HISTORIA DE AMOR ENTRE LA PUBLICIDAD CONDUCTUAL Y LA INTELIGENCIA ARTIFICIAL

La revolución digital y el desarrollo de nuevas plataformas de mercado crearon un terreno fértil para el desarrollo de un nuevo modelo económico: el basado en los datos. Aunque no es el único modelo económico que se ha desarrollado,[2] sin duda es el dominante en los mercados en línea.[3] En 2020, siete de las diez empresas más valiosas del mundo en términos de capitalización bursátil operaban, entre otras cosas, plataformas en línea.[4] Este rápido cambio en el poder económico llevó a algunos a considerar que "los datos son a este siglo lo que el petróleo fue al anterior".[5] En este modelo basado en los datos, las empresas tecnológicas prestan servicios gratuitos o de pago en línea a los consumidores. Esto les permite recopilar los datos personales de sus usuarios, generando enormes cantidades de información que suelen denominarse "big data".[6] A su vez, el análisis de los datos permite a las empresas desarrollar un sinfín de aplicaciones, a menudo basadas en la IA. Muchas de estas aplicaciones han tenido un profundo impacto en los consumidores en las últimas dos décadas. Las empresas alimentan sus sistemas de IA con estas grandes cantidades de datos para mejorar su rendimiento, sobre todo porque cuanto más complejos son los problemas que los sistemas de IA deben resolver, más datos necesitan. Este artículo se centra en el modelo económico basado en datos personales, a diferencia de otros tipos de datos como los industriales, por ejemplo.

---

[2] Piensa en modelos alternativos, colaborativos y sin ánimo de lucro, como el construido por Wikipedia.

[3] The Economist, "Data is giving rise to a new economy", 6 de mayo de 2017, https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy [consultado por última vez el 12 de octubre de 2021].

[4] Por orden de tamaño, estas empresas son Microsoft, Apple, Amazon, Alphabet, Facebook, Alibaba, Tencent Holdings (Statista, "The 100 largest companies in the world by market capitalization in 2020", disponible en: https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/). Todas ellas contratan con consumidores.

[5] The Economist, "Data is giving rise to a new economy", 6 de mayo de 2017, https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy [consultado por última vez el 12 de octubre de 2021].

[6] Según algunas estimaciones, en 2025 se crearán alrededor de 463 exabytes de datos al día en todo el mundo (World Economic Forum, "How much data is generated each day?", 17 de abril de 2019, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/ [consultado por última vez el 12 de octubre de 2021].

En este nuevo modelo económico, los datos sobre el comportamiento de los consumidores se volvieron fácilmente recopilables y procesables. Al principio, los datos de comportamiento se reutilizaban exclusivamente para mejorar los servicios de las empresas tecnológicas, lo que en última instancia beneficiaba a los consumidores. Por ejemplo, Google inicialmente sólo reinvertía los datos de comportamiento de sus usuarios para mejorar su motor de búsqueda y ofrecer resultados de búsqueda más precisos. Si los usuarios no tenían que pagar por el motor de búsqueda de Google, la empresa recogía sus datos de comportamiento para mejorar sus resultados de búsqueda. Shoshana Zuboff lo denominó "ciclo de reinversión del valor del comportamiento".[7] Sin embargo, la simple reinversión de los datos de comportamiento de los consumidores para mejorar el producto era una buena manera de crear y mejorar los servicios en línea, pero no era suficiente para generar beneficios.[8]

Esto explica por qué las empresas tecnológicas empezaron a utilizar esos datos de comportamiento para otros fines comerciales, principalmente la publicidad digital, que constituye la principal fuente de ingresos de Google y Facebook. De hecho, una gran parte de los sitios web obtienen la mayor parte de sus ingresos de la publicidad digital.[9] La publicidad también se ha descrito como la "savia de internet".[10] Basándose en el conocimiento de primera mano de sus usuarios, las empresas pueden vender no sus datos personales como tales, sino el acceso directo a ellos con fines de marketing. Los anunciantes pagan por el acceso a esa información para mostrar anuncios, ya sea en los sitios web propios de estas plataformas (por ejemplo, en los resultados de búsqueda de Google o en los *feeds* de noticias de Facebook) o en espacios publicitarios de sitios web de terceros, a categorías específicas de consumidores. Dado que Google y Facebook recogen y procesan masivamente información personal (declarada o inferida) sobre sus usuarios, pueden ofrecer una orientación publicitaria mucho más precisa que en los modelos publicitarios tradicionales. Aunque la publicidad digital será el tema central de este artículo, los datos personales también se recogen y procesan con otros fines. Los datos personales pueden comprarse y venderse para su uso en varias industrias para

[7] ZUBOFF, Shoshana (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile Books, pp. 69-70.

[8] ZUBOFF, Shoshana (2019: 69).

[9] ACQUISTI, Alessandro, TAYLOR, Curtis & WAGMAN, Liad (2016): "The Economics of Privacy", *Journal of Economic Literature*, 54(2), p. 463. http://dx.doi.org/10.1257/jel.54.2.442.

[10] COFONE, Ignacio & ROBERTSON, Adriana (2018): "Consumer Privacy in a Behavioral World", *Hastings Law Journal*, 69(6), pp. 1472. https://repository.uchastings.edu/hastings_law_journal/vol69/iss6/1.

alimentar los sistemas de IA, como el transporte,[11] la salud,[12] los servicios financieros,[13] etc. Sin embargo, como señalan Acquisti, Taylor y Wagman, "los datos personales se compran, se venden y se intercambian continuamente entre las empresas (desde las agencias de información crediticia hasta las empresas de publicidad, pasando por los llamados "infomediarios" que compran, venden e intercambian datos personales), pero los propios consumidores no tienen acceso a esos mercados".[14]

La capacidad de las empresas tecnológicas para rastrear a los consumidores en línea es clave para la recopilación de datos sobre el comportamiento.[15] En el ecosistema móvil, los desarrolladores de aplicaciones pueden incorporar rastreadores de terceros en el código fuente de las aplicaciones, lo que a su vez permite a estos terceros (como Google, Facebook, Amazon, Microsoft) rastrear a los usuarios no sólo en sus plataformas propias, sino también en todas las aplicaciones y dispositivos. El seguimiento por parte de terceros en el ecosistema móvil es muy común. Un estudio de casi un millón de aplicaciones de las tiendas Google Play de EE. UU. y el Reino Unido muestra que el 90,4% de ellas incorporan al menos un rastreador, mientras que el 17,9% contiene más de veinte.[16] Existen otras técnicas de rastreo, como las conocidas *cookies*,[17] el *fingerprinting*,[18] los identificadores de anuncios móviles[19] y el seguimiento de las direcciones IP. Los proveedores de servicios

---

[11] WAGNER, Ben, WINKLER, Till y HUMAN, Soheil (2021): "Bias in Geographic Information Systems: The Case of Google Maps", in *Proceedings of the 54th Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences. https://epub.wu.ac.at/id/eprint/7801.

[12] GRUSON, Damien, HELLEPUTTE, Thibault, ROUSSEAU, Patrick & GRUSON, David (2019) "Data science, artificial intelligence, and machine learning: Opportunities for laboratory medicine and the value of positive regulation", *Clinical Biochemistry*, 69, pp. 1-7. https://doi.org/10.1016/j.clinbiochem.2019.04.013.

[13] AGGARWAL, Nikita (2021): "The Norms of Algorithmic Credit Scoring", *The Cambridge Law Journal*, 80(1), pp. 42-73. https://doi.org/10.1017/S0008197321000015.

[14] ACQUISTI, Alessandro, TAYLOR, Curtis & WAGMAN, Liad (2016: 447).

[15] BINNS, R. *et al.* (2018): "Third Party Tracking in the Mobile Ecosystem", in *Proceedings of the 10th ACM Conference on Web Science*, pp. 23-31. https://doi.org/10.1145/3201064.3201089.

[16] Ibid.

[17] ENGLEHARDT, Steven & NARAYANAN, Arvind (2016): "Online tracking: A 1-million-site measurement and analysis", in *CCS 2016 - Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1388-1401. https://doi.org/10.1145/2976749.2978313.

[18] ACAR, Gunes, JUAREZ, Marc, NIKIFORAKIS, Nick *et al*. (2013). "FPDetective: Dusting the Web for Fingerprinters", en *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 1129-1140. https://doi.org/10.1145/2508859.2516674.

[19] En la actualidad, los sistemas operativos móviles (Android y iOS) adjuntan un identificador de publicidad móvil a cada dispositivo en el que operan, lo que hace posible que los anunciantes identifiquen individualmente el dispositivo de una persona y rastreen su actividad a través de las aplicaciones. Recientemente, Apple anunció que iba a exigir el consentimiento explícito de sus clientes para que se activara dicho identificador en sus dispositivos iOS, aunque ya existía la opción de desactivar la función (Apple, "Data Privacy Day at Apple: Improving transparency and empowering users", 27 de enero de 2021, https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-

de Internet también pueden controlar potencialmente toda la actividad en línea de sus clientes, estando "en la fuente".[20] El seguimiento es, por tanto, el núcleo de muchos modelos de negocio en línea. De hecho, los representantes de las industrias de los medios de comunicación y del marketing calculan que "están en juego miles de millones de dólares si el rastreo por parte de terceros termina sin atenuarse".[21] El siguiente paso en el rastreo de los consumidores es el desarrollo de la Internet de los objetos y las redes 5G, y la ubicuidad de los objetos y sensores conectados que permiten a las empresas tecnológicas recopilar aún más datos personales, como coches, relojes, timbres, neveras, dispositivos médicos o incluso etiquetas de localización.[22]

Gracias a estos rastreadores, las empresas pueden crear perfiles individualizados de los consumidores, especialmente cuando agregan esa información o la compilan con conjuntos de datos comprados en los mercados de datos. Los principales actores de los mercados de datos son los corredores de datos, que recogen o compran datos personales de los consumidores para revenderlos, principalmente con fines de marketing digital. Por ejemplo, Acxiom -un corredor de datos con sede en Estados Unidos- ofrece datos sobre 700 millones de consumidores en todo el mundo, con unos 5.000 puntos de datos para cada perfil.[23] Un conocimiento tan detallado permite a los profesionales que utilizan la IA elaborar sofisticados perfiles sobre sus clientes. A modo de ejemplo, Airbnb posee una patente que utiliza el aprendizaje automático para determinar la fiabilidad de una persona a partir de rasgos de comportamiento y personalidad obtenidos de cualquier tipo de documento, incluso de cuentas de redes sociales.[24] Este es solo un ejemplo de cómo los profesionales pueden ahora dirigirse a clientes individuales, personalizar sus productos, servicios y potencialmente toda la transacción con los consumidores (incluido el precio).

---

improving-transparency-and-empowering-users/ [consultado por última vez el 12 de octubre de 2021]). Esto creó una disputa pública con Facebook, uno de los principales rastreadores de terceros (The Economist, "Apple's duel with Facebook is a new form of big-tech rivalry", 27 de febrero de 2021, https://www.economist.com/business/2021/02/27/apples-duel-with-facebook-is-a-new-form-of-big-tech-rivalry [consultado por última vez el 12 de octubre de 2021].

[20] COFONE, Ignacio & ROBERTSON, Adriana (2018: 1473).

[21] Interactive Advertising Bureau, "The Socioeconomic Impact of Internet Tracking", febrero de 2020, https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf [consultado por última vez el 12 de octubre de 2021].

[22] Apple, "Apple introduces AirTag", 20 de abril de 2021, https://swww.apple.com/newsroom/2021/04/apple-introduces-airtag/ [consultado por última vez el 12 de octubre de 2021].

[23] Acxiom Corporation, Form 10-K filed with the United States Securities and Exchange Commission on May 25, 2018, https://www.sec.gov/Archives/edgar/data/733269/000073326918000016/a2018q410k.htm [consultado por última vez el 12 de octubre de 2021].

[24] BAVEJA, Sarabjit Singh, SARMA, Anish Das & DALVI, Nilesh (2015): "Determining trustworthiness and compatibility of a person" (U.S. Patent No. 9,070,088). *U.S. Patent and Trademark Office*. https://patents.google.com/patent/US9070088B1/en.

Este nuevo modelo económico basado en la recopilación y el uso de datos personales está perturbando profundamente a la sociedad en general.[25] Shoshana Zuboff acuñó el famoso término "capitalismo de vigilancia" para describir "un nuevo orden económico que reclama la experiencia humana como materia prima gratuita para prácticas comerciales ocultas de extracción, predicción y venta".[26] En este nuevo orden, los datos personales se consideran simplemente un activo en bruto que se puede recopilar y vender libremente con fines comerciales, tal y como hacen los corredores de datos (a menudo legalmente). La publicidad digital basada en datos de comportamiento ha desempeñado un papel fundamental en el desarrollo de este nuevo orden. En un reciente proyecto de informe de la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo sobre la propuesta de Ley de Servicios Digitales, la ponente Christel Schaldemose explicaba que "cree firmemente que la recopilación y el uso generalizados de los datos de los usuarios para ofrecer publicidad dirigida, microdirigida y basada en el comportamiento se ha salido de control".[27]

No cabe duda de que el desarrollo tecnológico y la digitalización han traído muchos avances positivos para los consumidores, que tienen acceso a un sinfín de nuevos servicios de forma gratuita, a cambio de sus datos personales. Pero estos aspectos positivos pueden tener un coste para los consumidores, especialmente en términos de privacidad y autonomía. De hecho, hay una mayor conciencia pública de la importancia de la privacidad[28] y de cómo las empresas tecnológicas interfieren en la autonomía de los consumidores con fines de marketing.[29] Como se explica en la siguiente sección, los actuales desarrollos de la IA afectan aún más a la autonomía del consumidor, y la publicidad digital desempeña un papel importante en ese proceso.

---

[25] Para el público, impactantes documentales han denunciado las consecuencias de la vigilancia masiva por parte de corporaciones y gobiernos por igual (*Terms and Conditions May Apply* (2013): dirigido por Cullen HOBACK), cómo la analítica de *big data* permitió a Cambridge Analytica manipular elecciones (*The Great Hack* (2019): dirigida por Karim AMER & Jehane NOUJAIM, disponible en Netflix), la influencia negativa de las redes sociales en los espacios sociales, políticos y culturales (*The Social Dilemma (2020)*: dirigida por Jeff ORLOWSKI, disponible en Netflix), y los peligros del reconocimiento facial y los sesgos en la toma de decisiones algorítmicas (*Coded Bias (2020)*: dirigida por Shalini KANTAYYA, disponible en Netflix).

[26] ZUBOFF, Shoshana (2019).

[27] European Parliament's Committee on the Internal Market and Consumer Protection, Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD), 28.5.2021, https://www.europarl.europa.eu/doceo/document/IMCO-PR-693594_EN.pdf.

[28] VÉLIZ, Carissa (2021): *Privacy is Power*, Bantam Press.

[29] *The Social Dilemma* (2020): dirigida por Jeff ORLOWSKI, disponible en Netflix.

III. LA AUTONOMÍA DEL CONSUMIDOR ESTÁ EN PELIGRO EN LA ERA DE LA PUBLICIDAD CONDUCTUAL DIRIGIDA POR LA INTELIGENCIA ARTIFICIAL

La pandemia de COVID-19 puso de manifiesto los efectos ambivalentes de las tecnologías digitales. Por un lado, la tecnología permitió a los trabajadores y a los ciudadanos (especialmente en los países desarrollados) seguir gestionando muchos aspectos de sus vidas con escasas interacciones físicas. La gente ha podido mantenerse en contacto con sus seres queridos, trabajar a distancia, comprar en línea y tratar con sus administraciones públicas de forma digital. Por otra parte, el mayor tiempo que se pasa en línea suele significar que se recogen más datos personales y consumidores están más expuestos a la publicidad digital. La pandemia también ha puesto de manifiesto una línea difusa entre el mundo *online* y el *offline*, o una cierta digitalización de nuestras experiencias analógicas, que implica consecuencias negativas en términos de privacidad. Por ejemplo, el uso omnipresente de los códigos QR. En muchos lugares, los antiguos menús de los restaurantes han desaparecido por completo para dar paso a menús digitalizados a los que sólo se puede acceder escaneando códigos QR pegados a las mesas. Muchos gobiernos han impuesto el uso de tarjetas sanitarias para acceder a los propios restaurantes, pero también a locales de ocio nocturno, peluquerías, centros comerciales, etc. Potencialmente, muchos profesionales que no tenían acceso a los datos personales de sus clientes antes de la pandemia tienen ahora acceso de primera mano a ellos, sin que la mayoría de los consumidores sean conscientes de ello.[30] Por lo tanto, no hay que limitar el análisis a la recogida de datos en línea, ya que nuestros datos personales se recogen cada vez más en cualquier tipo de entorno, por una gama más amplia de actores. Por ejemplo, las *cookies* y otras técnicas de rastreo pueden implementarse fácilmente en los menús de los restaurantes digitalizados, lo que significa que también se están recogiendo más datos personales cuando los consumidores hacen sus necesidades en el mundo analógico, y que estos nuevos actores pueden ahora dedicarse a la publicidad digital ellos mismos o vender nuevos espacios publicitarios digitales a terceros.

Mi argumento general es que los avances tecnológicos sin precedentes de la IA permiten a los comerciantes capturar la autonomía del consumidor en términos de preferencias, elección, toma de decisiones y bienestar. Esta pérdida de autonomía tiene lugar en dos niveles principales: (i) antes de cualquier transacción; y (ii) al nivel de la propia transacción subyacente. Aquí nos centraremos en el papel de la publicidad digital en este proceso.

---

[30] WOO, Erin, "QR Codes Are Here to Stay. So Is the Tracking They Allow", *New York Times*, 26 de julio de 2021, https://www.nytimes.com/2021/07/26/technology/qr-codes-tracking.html [consultado por última vez el 12 de octubre de 2021].

Antes de realizar una transacción, los consumidores son objeto de perfiles y de publicidad individualizada. Contractualmente, esto es posible porque aceptan las condiciones de servicio y las políticas de privacidad de los sitios web y las aplicaciones. El principal problema en términos de autonomía privada comienza en el nivel de la recogida y el tratamiento de datos, antes de la transacción subyacente. Desde el principio, es importante señalar que los consumidores no siempre se dan cuenta de las implicaciones de sus decisiones antes de cualquier transacción subyacente. Al aceptar que se recojan las *cookies* y, en general, sus datos personales, no siempre comprenden plenamente que estos datos se utilizan para la publicidad dirigida y otros fines. Del mismo modo, ignoran quién tendrá posteriormente acceso a sus datos personales en los mercados de datos. En otras palabras, si los datos personales de los consumidores se utilizan en primer lugar con fines publicitarios, los consumidores pierden esencialmente el control sobre sus datos, que son utilizados con otros fines por agentes inesperados, de forma no transparente. Por lo tanto, la cuestión de la regulación de la publicidad digital es crucial para preservar la autonomía y la privacidad de los consumidores. Podría decirse que el uso de los datos personales en formas que los consumidores no esperaban permite a los comerciantes manipular el comportamiento tanto exógena como endógenamente, incluso antes de cualquier transacción subyacente (por ejemplo, la venta de bienes o servicios).

De forma exógena, los comerciantes pueden manipular el comportamiento gracias al acceso a los datos de comportamiento y al análisis predictivo. Un estudio reciente realizado en Viena sugiere que Google Maps influye en la elección del mejor tipo de transporte por parte de los usuarios, empujándolos a conducir su coche.[31] Es fácil imaginar cómo Google, uno de los principales actores del sector de la publicidad digital, podría utilizar su capacidad de influir en los consumidores para empujarlos a utilizar los servicios de transporte en coche anunciados en Maps, por ejemplo. Facebook, otro de los principales actores de la industria de la publicidad digital, demostró en un estudio que podía manipular las emociones de sus usuarios sin que estos fueran conscientes de ello.[32] Del mismo modo, los investigadores desarrollaron técnicas automatizadas para identificar patrones oscuros (*"dark patterns"*) en unos 11.000 sitios web de compras.[33] El estudio define los patrones oscuros como "opciones de diseño de la interfaz de usuario que benefician a un servicio en línea coaccionando, dirigiendo o engañando a los usuarios para

[31] WAGNER, Ben, WINKLER, Till y HUMAN, Soheil (2021).

[32] KRAMER, Adam, GUILLORY, Jamie & HANCOCK, Jeffrey (2014): "Experimental evidence of massive-scale emotional contagion through social networks", in *Proceedings of the National Academy of Sciences*, 111 (24) 8788-8790, https://doi.org/10.1073/pnas.1320040111.

[33] MATHUR, Arunesh *et al.* (2019): "Dark patterns at scale: Findings from a crawl of 11K shopping websites", in *Proceedings of the ACM on human-computer interaction*, 3(CSCW), pp. 1–32. https://doi.org/10.1145/3359183.

que tomen decisiones no deseadas y potencialmente perjudiciales". Los autores descubrieron que alrededor del 11% de estos sitios web contenían patrones oscuros, y que es más probable que aparezcan en sitios web populares. El Consejo Noruego del Consumidor había publicado anteriormente un informe que mostraba cómo las empresas tecnológicas utilizan los patrones oscuros para extraer grandes cantidades de datos personales de los consumidores.[34] La capacidad de las redes sociales y otras empresas tecnológicas para manipular las emociones a través de señales subliminales es, por tanto, real y podría utilizarse con fines de publicidad digital. Sin embargo, la reglamentación no aborda actualmente esta cuestión de forma adecuada, como explicado a continuación.

De forma endógena, esta falta de regulación y el aumento de la conciencia entre los consumidores de que su intimidad se está intercambiando por el acceso a productos y servicios gratuitos significa que algunos podrían autocensurarse debido al temor de la vigilancia comercial. Ambos tipos de manipulación del comportamiento tienen repercusiones negativas en el buen funcionamiento del mercado interior de la UE, por lo que se justifica una mayor intervención reguladora, como se argumenta en la sección 0.

A continuación, el nivel de la transacción subyacente, el conocimiento adquirido por los consumidores y la influencia ejercida sobre ellos en sentido ascendente permite a los comerciantes crear herramientas para automatizar las transacciones (ejerciendo potencialmente una gran influencia en las decisiones de compra) y realizar una discriminación de precios para cada cliente individual. Así, la influencia de la publicidad conductual en sentido ascendente puede tener efectos sobre las transacciones posteriores en sentido descendente. Aunque la posibilidad de la contratación automatizada y la discriminación de precios en la era de la IA requiere más investigación, este artículo se centra en el nivel ascendente de la elaboración de perfiles en línea y la publicidad conductual.

IV. INEFICACIA DEL ENFOQUE NORMATIVO TRADICIONAL

En este contexto, cabe preguntarse si el régimen normativo actual es suficiente para proteger a los consumidores, especialmente en términos de privacidad y autonomía. Este artículo sostiene que, a pesar de la entrada en vigor del Reglamento General de Protección de Datos (RGPD)[35] en mayo de 2018, el actual marco normativo no protege

[34] FROBRUKERRÅDET (2018). *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[35] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), OJ L 119, 4.5.2016, p. 1–88.

adecuadamente a los consumidores de los efectos negativos de la publicidad conductual descritos anteriormente. Esto se debe a que los conceptos tradicionales de consentimiento, transparencia y control han resultado esencialmente ineficaces.

4.1. Consentimiento

De entrada, conviene señalar que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea establece el derecho a la protección de los datos personales. Su segundo apartado exige que el tratamiento de los datos personales se base en el consentimiento del interesado, o en alguna otra base legítima establecida por la ley. El RGPD establece seis bases jurídicas para el tratamiento de datos personales.[36] Tres de ellas son pertinentes en el contexto de la publicidad conductual: (i) el consentimiento;[37] (ii) la necesidad para la ejecución de un contrato; [38]y (iii) la necesidad para los fines de un interés legítimo perseguido por el responsable del tratamiento o por un tercero.[39] El RGPD establece condiciones estrictas para el consentimiento: debe ser "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".[40]

El Tribunal de Justicia de la Unión Europea (TJUE) ha especificado estos requisitos de consentimiento en su jurisprudencia, incluso en relación con la publicidad digital. Por ejemplo, en virtud de la Directiva sobre la privacidad y las comunicaciones electrónicas (que también es pertinente cuando se almacenan en el dispositivo piezas de seguimiento como las cocinadas)[41], leída conjuntamente con los requisitos de consentimiento del RGPD, el consentimiento no es válido si las *cookies* se almacenan en el dispositivo de un usuario de un sitio web a través de una casilla de verificación previamente marcada que el usuario debe deseleccionar para denegar su consentimiento, independientemente de si se trata de datos personales o no: " Debe ser claramente comprensible y suficientemente

---

[36] Artículo 6 del RGPD.

[37] Artículo 6(1)(a) del RGPD.

[38] Artículo 6(1)(b) del RGPD.

[39] Artículo 6(1)(f) del RGPD.

[40] Artículo 4(11) del RGPD. Véase también el considerando 32 y el artículo 7 del RGPD, que establecen condiciones más detalladas y el derecho del interesado a retirar su consentimiento en cualquier momento.

[41] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, DO L 201 de 31.7.2002, p. 37.

detallada para que el usuario pueda comprender el funcionamiento de las *cookies* empleadas".[42] Del mismo modo, los sitios web que incorporan módulos sociales de terceros deben obtener el consentimiento de sus visitantes.[43] Además, el interesado debe ser capaz de comprender las consecuencias de su consentimiento, de modo que éste se dé con pleno conocimiento de causa; por ello, debe recibir información relativa a todas las circunstancias que rodean ese tratamiento, de forma inteligible y fácilmente accesible, utilizando un lenguaje claro y sencillo.[44] El Comité Europeo de Protección de Datos también adoptó directrices sobre el consentimiento en el marco del RGPD en mayo de 2020.[45]

Desde la entrada en vigor del RGPD, las autoridades europeas de protección de datos (APD) han multado a varias empresas por no cumplir con estos estrictos requisitos de consentimiento en el contexto de la publicidad dirigida. Por ejemplo, la CNIL (la APD francesa) impuso una multa de 50 millones de euros a Google en 2019 por no obtener el consentimiento válido de sus usuarios a efectos de la publicidad personalizada,[46] confirmada posteriormente por el Consejo de Estado francés.[47] El regulador consideró que el consentimiento de los usuarios no estaba suficientemente informado porque la información de que la empresa trataría los datos personales para la personalización de los anuncios no estaba centralizada en un documento y los usuarios no sabrían que su información sería tratada con ese fin utilizando los numerosos servicios de Google. El consentimiento tampoco era inequívoco porque la opción de que se mostraran anuncios personalizados estaba marcada previamente en una configuración difícil de encontrar. Por último, el consentimiento tampoco era específico, porque Google solicitaba el consentimiento cuando los usuarios creaban una cuenta, marcando las casillas para aceptar sus condiciones de servicio y su política de privacidad, mientras que el consentimiento debería obtenerse de forma diferenciada para cada fin. Recientemente,

---

[42] Sentencia de 1 de octubre de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV contra Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, apartado 74.

[43] Sentencia de 29 de julio de 2019, *Fashion ID GmbH & Co. KG contra Verbraucherzentrale NRW eV*, C-40/17 ECLI:EU:C:2019:629.

[44] Sentencia de 11 de noviembre de 2020, *Orange România SA contra Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, C-61/19, ECLI:EU:C:2020:901, apartado 52.

[45] Véanse las Directrices 05/2020 sobre el consentimiento en virtud del Reglamento 2016/679 Versión 1.1, adoptadas el 4 de mayo de 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [consultado por última vez el 12 de octubre de 2021].

[46] Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2019-001 du 21 janvier 2019, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/.

[47] Conseil d'Etat, décision n°430810 du 19 juin 2020, ECLI:FR:CECHR:2020:430810.20200619.

también multó al periódico Le Figaro con 50.000 euros por colocar *cookies* publicitarias en su página web sin obtener el consentimiento del usuario.[48] Entre 2020 y 2021, la CNIL adoptó alrededor de 70 medidas correctivas (avisos formales y sanciones) relacionadas con el incumplimiento de la normativa sobre *cookies*, especialmente relacionadas con el consentimiento.[49] Al parecer, la DPA belga está investigando a IAB Europe (la asociación de la industria del marketing y la publicidad digital) por sospechas de que su llamado "marco de transparencia y consentimiento", que los editores web utilizan para buscar el consentimiento, no cumple con los requisitos de consentimiento del RGPR.[50] Fuera de la UE, el Tribunal Federal de Australia también determinó que Google seguía recopilando datos de localización de los dispositivos Android aunque los usuarios hubieran desactivado la configuración del "historial de localización", eludiendo así por completo el consentimiento del consumidor,[51] aunque los datos de localización pueden ser relevantes para fines publicitarios personalizados.

A veces, el consentimiento se obtiene de forma indirecta. Es el caso de Facebook, que procesa los datos de sus usuarios y ofrece publicidad personalizada no sobre la base legal del "consentimiento" (artículo 6.1.a del RGPD), sino sobre la base de la "necesidad para la ejecución de un contrato" (artículo 6.1.b del RGPD). El activista Max Schrems presentó un caso contra Facebook sobre este punto en Austria, que llegó al TJUE a través de un procedimiento prejudicial en julio de 2021.[52] Considera que la elección por parte de Facebook de esta base jurídica para el tratamiento de datos en el marco del RGPD perjudica a sus usuarios, ya que la base jurídica del "consentimiento" ofrece un mayor nivel de protección, mientras que el consentimiento que se solicita a través de las condiciones generales de servicio de Facebook -que los usuarios apenas leen- no permite que se otorgue de forma libre, específica e inequívoca. El TJUE tendrá que responder a la pregunta de si Facebook puede efectivamente basarse en el artículo 6.1.b) en lugar del

---

[48] Comisión Nacional de la Informática y las Libertades, Decreto SAN-2021-013 del 27 de julio de 2021, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043867129.

[49] Commission Nationale de l'Informatique et des Libertés, "Refuser les cookies doit être aussi simple qu'accepter : bilan de la deuxième campagne de mises en demeure et actions à venir", 14 de septiembre de 2021, https://www.cnil.fr/fr/refuser-les-cookies-doit-etre-aussi-simple-quaccepter-bilan-de-la-deuxieme-campagne-de-mises-en.

[50] NEWMAN, Matthew, "IAB Europe's GDPR probe moves forward in hearing with Belgian authority", *MLex*, 25 de junio de 2021, https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/iab-europes-gdpr-probe-moves-forward-in-hearing-with-belgian-authority [consultado por última vez el 12 de octubre de 2021].

[51] Australian Competition and Consumer Commission, "Google misled consumers about the collection and use of location data", 16 de abril de 2021, https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data [consultado por última vez el 12 de octubre de 2021].

[52] Véase la petición de decisión prejudicial en el asunto C-446/21.

artículo 6.1.a) del RGPD para tratar los datos personales de sus usuarios en el contexto de la publicidad personalizada solicitando su consentimiento en sus condiciones de servicio.[53] Aunque el caso parece similar al que la APD francesa multó a Google en 2019 por no obtener un consentimiento válido, un proyecto de decisión de la APD irlandesa sugiere que permitiría a Facebook basarse en el artículo 6(1)(b) del GDPR para obtener el consentimiento de sus usuarios, pero seguiría multando a la red social por no haber sido totalmente transparente sobre el cambio de base legal.[54]

En un artículo reciente, Michael Veale y Frederik Zuiderveen Borgesius sostienen que el consentimiento es la única base jurídica adecuada para las ofertas en tiempo real, una forma habitual de realizar publicidad basada en el comportamiento en línea mediante procesos de subasta.[55] Argumentan que la base jurídica de la "necesidad de ejecución de un contrato" no es apropiada porque los usuarios de Internet no visitan los sitios web con la intención de utilizar el servicio a cambio de un seguimiento y una publicidad de puja en tiempo real (que, como explican, implica una compleja red de terceros).[56] En definitiva, los autores argumentan que las pujas en tiempo real no cumplen con los requisitos de consentimiento establecidos por el RGPD porque (i) el consentimiento no puede ser retirado; (ii) los mecanismos de consentimiento global utilizados para señalar el consentimiento a través de los sitios web con fines de pujas en tiempo real serían incompatibles con la jurisprudencia del TJUE sobre el control conjunto y comprometen la responsabilidad de los editores; y (iii) la infraestructura de las pujas en tiempo real implica a demasiadas partes para que el consentimiento sea válido.[57]

Sin embargo, se podría argumentar que, incluso si se obtuviera legalmente con arreglo al precepto del RGPD, el consentimiento sería insuficiente para proteger eficazmente a los consumidores y garantizar su derecho fundamental a la protección de sus datos

---

[53] La sección 2 de las condiciones del servicio de Facebook dice " En lugar de pagar por usar Facebook y el resto de los productos y servicios que ofrecemos, al usar los Productos de Facebook que se incluyen en estas Condiciones, aceptas que podamos mostrarte anuncios de las empresas y organizaciones que nos pagan por promocionarse dentro y fuera de los Productos de las empresas de Facebook. Usamos tus datos personales, como la información sobre tu actividad y tus intereses, para mostrarte aquella publicidad que pueda resultarte más relevante" [última revisión: 20 de diciembre de 2020; último acceso: 12 de octubre de 2020].

[54] NOYB, "Irish DPC greenlights Facebook's "GDPR bypass". Schrems: "Decision undermines key element of GDPR", 13 de octubre de 2021, https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass [consultado por última vez el 13 de octubre de 2021].

[55] VEALE, Michael & ZUIDERVEEN BORGESIUS, Frederik, (2021, de próxima aparición): "Adtech and Real-Time Bidding under European Data Protection Law", *German Law Journal*. https://doi.org/10.31235/osf.io/wg8fq.

[56] Ibid, p. 17.

[57] VEALE, Michael & ZUIDERVEEN BORGESIUS, Frederik, (2021, de próxima aparición: 23-29).

personales, al menos por tres razones.[58] En primer lugar, cuando se trata de datos personales, los consumidores suelen enfrentarse a la "paradoja de la privacidad" (*"privacy paradox"*): aunque declaran constantemente que valoran la privacidad, a menudo no actúan para protegerla y facilitan libremente sus datos.[59] La paradoja de la privacidad se agudiza aún más cuando los datos personales se difunden en mayor cantidad. Con el desarrollo del Internet de los objetos, el aumento del uso de Internet y la mayor digitalización de nuestras vidas durante la pandemia, se podría temer que esta paradoja se profundice. En este contexto, sugerir que las personas no se preocupan por su privacidad porque no están dispuestas a pagar por ella[60] o porque deciden libremente ceder sus datos personales (por ejemplo, aceptando condiciones de servicio) es ignorar sin tapujos la paradoja de la privacidad.

En segundo lugar, los consumidores parecen sufrir un sesgo cognitivo conocido como la "no creencia en la ley de los grandes números" *("non-belief in the law of large numbers"*), según el cual, debido a la sobrecarga de información sobre las implicaciones de sus decisiones en materia de privacidad, en realidad la infravaloran.[61] Este podría ser el caso de las inferencias realizadas por los sistemas de IA y utilizadas posteriormente para la publicidad conductual. Por ejemplo, al subir una foto a Instagram, un usuario puede no ser plenamente consciente de que, por defecto, la aplicación tiene acceso a toda su biblioteca de fotos, que los metadatos de cada foto pueden utilizarse para inferir información sobre su información más sensible, que esta decisión también implica a las personas que etiquetan, y que toda esa información personal será utilizada por una miríada de actores de la tecnología publicitaria con fines de publicidad conductual dirigida. Todas las ramificaciones de subir una simple foto son demasiado complejas. Esto conduce a un fallo del mercado porque la privacidad del consumidor en los mercados alcanza niveles ineficientemente bajos.

En tercer lugar, los derechos de privacidad del RGPD (propiedad de los datos, accesibilidad y portabilidad) solo tienen en cuenta los datos que se han proporcionado, no los datos que se han generado o inferido gracias a esos datos y en base a ellos.[62] En otras palabras, el consentimiento no sólo es defectuoso para los datos proporcionados, sino que

---

[58] Tal y como establece el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

[59] NORBERG, Patricia, HORNE, Daniel, & HORNE, David (2007): "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *Journal of Consumer Affairs*, 41(1), pp. 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x; ACQUISTI, Alessandro, TAYLOR, Curtis & WAGMAN, Liad (2016: 476).

[60] BEN-SHAHAR, Omri y STRAHILEVITZ, Lior (2016: 5).

[61] COFONE, Ignacio & ROBERTSON, Adriana (2018: 1475).

[62] ZUBOFF, Shoshana (2019: 480-488).

es inexistente para los datos inferidos. Podría decirse que los datos inferidos son incluso más poderosos o útiles que los datos declarados explícitamente cuando los *big data* y la IA permiten realizar determinaciones probabilísticas. Esto ha llevado a los expertos en ética a pedir que se establezca un nuevo derecho de protección de datos: el derecho a las inferencias razonables.[63]

4.2. Transparencia

Tradicionalmente se ha recurrido a la transparencia en la regulación de la protección de los consumidores, basándose en el supuesto de que los consumidores son agentes racionales que leen la información y son capaces de tomar decisiones con conocimiento de causa. La obligación de divulgación también se percibe a veces como una herramienta reguladora relativamente barata y no intrusiva, especialmente en Estados Unidos.[64] En los mercados de datos personales, el RGPD sigue basándose en los requisitos de transparencia. La transparencia es uno de los principios clave aplicables al tratamiento de datos personales.[65] El Reglamento impone obligaciones de transparencia a los responsables del tratamiento a la hora de proporcionar información a los interesados,[66] incluso cuando se someten a la elaboración de perfiles y las consecuencias de dicha elaboración.[67] En lo que respecta a este artículo, el considerando 58 del RGPD sobre la transparencia hace una referencia explícita a la publicidad en línea, afirmando que la transparencia es especialmente pertinente en situaciones "en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad".

Sin embargo, a pesar de que algunos estudiosos del derecho privado siguen viendo los requisitos de transparencia como una posible solución para proteger la privacidad de los consumidores,[68] la investigación sigue demostrando que las divulgaciones obligatorias no protegen eficazmente a los consumidores o incluso pueden perjudicarlos en algunos

---

[63] WACHTER, Sandra & MITTELSTADT, Brent (2019): “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI”, *Columbia Business Law Review*, 2019(2), pp. 1-130.

[64] SCHNEIDER, Carl E. & BEN-SHAHAR, Omri (2010): "The Failure of Mandated Disclosure", *John M. Olin Program in Law and Economics Working Paper No. 516*, https://chicagounbound.uchicago.edu/law_and_economics/520/, p. 24.

[65] Artículo 5(1)(a) del RGPD.

[66] Artículo 12(1) del RGPD.

[67] Considerando 60 y artículo 14(2)(g) del RGPD.

[68] COFONE, Ignacio & ROBERTSON, Adriana (2018: 1503).

casos.[69] Apoyadas por la investigación empírica, estas conclusiones son válidas en contextos de contratación en línea, lo que sugiere que ninguna minoría informada sería capaz de disciplinar a los vendedores para que redacten condiciones favorables para los consumidores.[70] Esto ha llevado a algunos autores a argumentar que la regulación de la protección de los consumidores y de los datos debería seguir el ritmo del desarrollo de los *big data* y de los algoritmos, y prever una información personalizada y adaptada a cada individuo.[71]

Además, el ideal de transparencia también ha sido criticado en el contexto algorítmico porque los sistemas algorítmicos y de IA carecen intrínsecamente de transparencia, lo que los protege del escrutinio público.[72] Esto se conoce comúnmente como el problema de la "caja negra" (*"black box"*).[73] En ese contexto, los consumidores suelen ignorar la base de las recomendaciones en línea, lo que a su vez podría persuadirles de consumir cosas que no habrían consumido si hubieran entendido la base de dichas recomendaciones. Y lo que es peor, incluso si las empresas tecnológicas cumplieran todos los requisitos de transparencia, los consumidores parecen estar mal equipados para comprender plenamente las explicaciones de los profesionales sobre el uso de sus datos personales (por ejemplo, con fines de publicidad conductual) y sus consecuencias en las decisiones algorítmicas posteriores, lo que pone de manifiesto una especie de "falacia de la transparencia" *("transparency fallacy")*.[74] El desarrollo de las tecnologías de aprendizaje profundo hace ahora imposible comprender plenamente los razonamientos algorítmicos que se basan en miles de millones de parámetros.

---

[69] SCHNEIDER, Carl E. & BEN-SHAHAR, Omri (2010); BEN-SHAHAR, Omri & SCHNEIDER, Carl E. (2014). *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton University Press.

[70] MAROTTA-WURGLER, Florencia (2011): "Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's 'Principles of the Law of Software Contracts'", *University of Chicago Law Review*, 78(1), pp. 165-186; BAKOS, Yannis, MAROTTA-WURGLER, Florencia & TROSSEN, David (2014): "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts", *The Journal of Legal Studies*, 43(1), pp. 1–35.

[71] BUSCH, Christoph (2019): "Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law", *The University of Chicago Law Review*, 86, pp. 309-331; BEN-SHAHAR, Omri & PORAT, Ariel (2021): *Personalized Law*, Oxford University Press (véase Chapter 5: Personalized Regulatory Techniques).

[72] ANNANY, Mike & CRAWFORD, Kate (2016): "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability", *New Media & Society*, 20(3), pp. 973-989, https://doi.org/10.1177%2F1461444816676645. Carissa Véliz argumenta: "Sólo podemos regular los anuncios si podemos verlos, por lo que los anuncios oscuros y personalizados tienen que desaparecer" (VÉLIZ, Carissa [2021: 108]).

[73] MARTINI, Mario (2020): "Regulating Algorithms: How to Demystify the Alchemy of Code?" in EBERS, Martin & NAVAS, Susana (Eds.), *Algorithms and Law* (pp. 100-135), Cambridge University Press. https://doi.org/10.1017/9781108347846.004.

[74] EDWARDS, Lilian & VEALE, Michael (2017): "Slave to the Algorithm", *Duke Law and Technology Review*, 16(1), p. 67.

La transparencia parece aún más ineficaz para proteger a los consumidores en línea cuando se utilizan patrones oscuros para engañarlos y hacer que divulguen más datos personales. Las empresas que utilizan patrones oscuros parecen cumplir formalmente con los requisitos de divulgación, pero en realidad utilizan estos requisitos normativos para manipular a los consumidores. La investigación empírica muestra que los llamados "*banners* de *cookies*" que aparecen en los sitios web para solicitar el consentimiento de los consumidores para colocar *cookies* en sus dispositivos no cumplen, en su mayoría, con el RGPD.[75] En concreto, los autores descubrieron que, de los datos desechados de los 10.000 sitios web más importantes del Reino Unido, solo el 11,8% cumple los requisitos del RGPD para obtener un consentimiento válido. En este caso, la transparencia y el consentimiento van de la mano, ya que los titulares de los datos sólo pueden dar su consentimiento válido si las empresas les informan debidamente de los fines del tratamiento de sus datos de forma inteligible. Los patrones oscuros, como los identificados en este estudio empírico -que burlan los requisitos de transparencia- hacen que el consentimiento no sea válido.

Estas conclusiones son relevantes en el contexto de la publicidad basada en el comportamiento, ya que los anuncios basados en la puja en tiempo real, por ejemplo, hacen un gran uso del consentimiento inválido que se busca gracias a los *banners* poco transparentes. Al igual que argumentaron que las empresas dedicadas a la puja en tiempo real no cumplen con los requisitos de consentimiento del RGPD, Michael Veale y Frederik Zuiderveen Borgesius también argumentan que no cumplen con sus requisitos de transparencia.[76] Y lo que es peor, explican por qué no sería posible que las pujas en tiempo real, en su forma actual, las cumplieran. Esto se debe a que los editores de sitios web no pueden predecir de antemano quién ganará la subasta de los anuncios mostrados en su sitio web y, por tanto, no pueden informar adecuadamente a sus visitantes sobre quién recogerá sus datos personales. La complejidad y los miles de actores que intervienen en esa industria también dificultan, si no impiden, que las pujas en tiempo real cumplan con los requisitos de transparencia del RGPD, porque los consumidores no son capaces de entender sus mecanismos. Esto es cierto, según los autores, independientemente de que los editores de sitios web y las empresas que participan en las pujas en tiempo real se consideren controladores conjuntos o no. De hecho, el propio sector teme que la adopción

[75] NOUWENS, Midas, LICCARDI, Ilaria, VEALE, Michael, KARGER, David & KAGAL, Lalana (2020): "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery*, pp. 1-13. https://doi.org/10.1145/3313831.3376321.

[76] VEALE, Michael & ZUIDERVEEN BORGESIUS, Frederik, (2021, de próxima aparición: 31-33).

de un nuevo Reglamento sobre la privacidad y las comunicaciones electrónicas[77] menoscabe su capacidad para realizar ofertas en tiempo real.[78] Por suerte, la transparencia aplicada a la administración pública permitió acceder a documentos de los grupos de presión de la industria ante la Comisión Europea en el que sus representantes expresaban estas preocupaciones.[79] Por el contrario, Facebook bloqueó recientemente a los investigadores del Ad Observatory de la Universidad de Nueva York que trabajan en la transparencia publicitaria,[80] y al organismo de control alemán AlgorithmWatch, por motivos similares.[81]

4.3. Control

Por último, parece que los consumidores siguen careciendo de control sobre sus datos personales una vez recogidos. Sin duda, el RGPD establece o codifica derechos destinados a proporcionar a los interesados un mayor control sobre sus datos: el derecho de acceso,[82] el derecho de rectificación,[83] el derecho al olvido,[84] el derecho a la limitación del tratamiento,[85] el derecho a la portabilidad de los datos,[86] el derecho de oposición[87] o el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles.[88] Muchos de estos derechos son relevantes en el contexto de la publicidad dirigida, especialmente este último, aunque no

---

[77] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017, COM/2017/010 final - 2017/03 (COD).

[78] RYAN, Johnny, “New evidence to regulators: IAB documents reveal that it knew that real-time bidding would be “incompatible with consent under GDPR”, *Brave*, February 20, 2021, https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/ [consultado por última vez el 12 de octubre de 2021].

[79] Ibid.

[80] Facebook, comunicado de prensa: "Research Cannot Be the Justification for Compromising People's Privacy", 3 de agosto de 2021, https://about.fb.com/news/2021/08/research-cannot-be-the-justification-for-compromising-peoples-privacy/ [consultado por última vez el 12 de octubre de 2021].

[81] AlgorithmWatch, comunicado de prensa: "AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook", 13 de agosto de 2021, https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook/ [consultado por última vez el 12 de octubre de 2021].

[82] Artículo 15 del RGPD.

[83] Artículo 16 del RGPD.

[84] Artículo 17 del RGPD.

[85] Artículo 18 del RGPD.

[86] Artículo 20 del RGPD.

[87] Artículo 21 del RGPD.

[88] Artículo 22 del RGPD.

se aplica si la toma de decisiones automatizada es necesaria para celebrar o ejecutar un contrato entre el interesado y un responsable del tratamiento o se basa en el consentimiento explícito del interesado. En la práctica, estas excepciones reducen drásticamente el ámbito de aplicación de dicha disposición, lo que ha llevado a algunos autores a reclamar su reformulación radical en la era de la IA.[89] Curiosamente, el TJUE aún no ha emitido ninguna sentencia sobre esta disposición. El RGPD también impone obligaciones a los responsables y encargados del tratamiento en materia de seguridad,[90] notificación de las violaciones de los datos personales a las autoridades de control[91] y comunicación de dichas violaciones a los interesados.[92] Sin embargo, parece que estos derechos no son suficientemente efectivos, al menos por tres razones.

En primer lugar, el anonimato es muy difícil, si no imposible, de conseguir. Obviamente, todos estos derechos mencionados anteriormente sólo se aplican cuando el propio Reglamento es aplicable, es decir, cuando los datos se consideran personales.[93] Pero según el RGPD, los datos no deben considerarse personales si se anonimizan.[94] Por lo tanto, grandes conjuntos de datos considerados anónimos están siendo utilizados por los profesionales (incluso en la industria de la tecnología publicitaria) sin aplicar los principios del RGPD porque los consideran anónimos. Sin embargo, los estudios empíricos demuestran sistemáticamente que el anonimato de los datos es casi una ilusión. Por ejemplo, los investigadores pudieron reidentificar de forma exclusiva a los individuos el 95% de las veces basándose en un conjunto de datos que contenía datos de movilidad por hora de 1,5 millones de individuos.[95] El estudio explica que "la geolocalización de ~50%

[89] DE HERT, Paul & LAZCOZ, Guillermo (2021): "Radical rewriting of Article 22 GDPR on machine decisions in the AI era", *European Law Blog*, https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/ [consultado por última vez el 13 de octubre de 2021].

[90] Artículo 32 del RGPD.

[91] Artículo 33 del RGPD.

[92] Artículo 34 del RGPD.

[93] Véase el artículo 2, apartado 1, del RGPD. El artículo 4, apartado 1, define los datos personales como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

[94] El considerando 26 del RGPD establece: "[...] Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo."

[95] DE MONTJOYE, Yves-Alexandre, HIDALGO, César, VERLEYSEN, Michel & BLONDEL, Vincent (2013): “Unique in the Crowd: The Privacy Bounds of Human Mobility”, *Scientific Reports*, 3:1376. https://doi.org/10.1038/srep01376.

de todo el tráfico de iOS y Android si está disponible para las redes publicitarias".[96] Del mismo modo, los investigadores fueron capaces de reidentificar de forma única al 90% de los individuos al realizar un estudio de 3 meses basado en los registros de tarjetas de crédito de 1,1 millones de individuos, basándose únicamente en cuatro puntos espacio-temporales.[97] Los autores concluyen que sus resultados "ponen de manifiesto la necesidad de reformar nuestros mecanismos de protección de datos más allá de la [información personal identificable] y el anonimato y hacia una evaluación más cuantitativa de la probabilidad de reidentificación".[98] También es posible utilizar un modelo estadístico para reidentificar a individuos únicos en conjuntos de datos muy incompletos: un estudio muestra que el 99,98% de los estadounidenses pueden ser reidentificados basándose en ese modelo, gracias a cualquier conjunto de datos que contenga 15 atributos demográficos.[99] Los autores concluyen que es poco probable que tales conjuntos de datos cumplan con el RGPD. Por último, otro estudio demuestra que el riesgo de reidentificación solo disminuye lentamente a medida que aumenta el tamaño de los conjuntos de datos, confirmando así las conclusiones anteriores incluso para los conjuntos de datos a escala nacional.[100] Estos estudios muestran sistemáticamente que la anonimización es difícil, si no imposible, en la era de los *big data*. Desde un punto de vista jurídico, esto significa que los principios y derechos del RGPD deberían aplicarse probablemente a más conjuntos de datos de lo que es el caso actualmente.

En segundo lugar, la dificultad para anonimizar los conjuntos de datos hace que su protección sea aún más importante. Sin embargo, continuamente salen a la luz importantes violaciones de datos.[101] Aparte de emprender una acción por daños y perjuicios contra el responsable del tratamiento, los consumidores pierden el control sobre esos datos violados. Incluso cuando los datos no han sido violados, cuando los consumidores piden a las redes sociales u otras plataformas que eliminen sus datos,[102] no

---

[96] Ibid, p. 1.

[97] DE MONTJOYE, Yves-Alexandre, RADAELLI, Laura, KUMAR SINGH, Vivek & PENTLAND, Alex 'Sandy' (2015): "Unique in the shopping mall: On the reidentifiability of credit card metadata", *Science*, 347(6221), https://doi.org/10.1126/science.1256297, pp. 536-539.

[98] Ibid, p. 539.

[99] ROCHER, Luc, HENDRICKX, Julien M. & DE MONTJOYE, Yves-Alexandre (2019): "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications*, 10(3069), https://doi.org/10.1038/s41467-019-10933-3.

[100] FARZANEHFAR, Ali, HOUSSIAU, Florimond & DE MONTJOYE, Yves-Alexandre (2021): "The risk of re-identification remains high even in country-scale location datasets", *Patterns*, 2(3): 100204, https://doi.org/10.1016/j.patter.2021.100204.

[101] PAUL, Kari, "Facebook says a breach that hit 533m is old news. Experts disagree", *Guardian*, 6 de abril de 2021, https://www.theguardian.com/technology/2021/apr/06/facebook-breach-data-leak [consultado por última vez el 12 de octobre de 2021].

[102] Hacer uso de su derecho al olvido en virtud del artículo 17 del RGPD.

tienen ninguna garantía de que sus datos se eliminen completamente de los sistemas de las empresas, o de que los algoritmos dejen de alimentarse con esos datos. Mientras tanto, es posible que esos datos ya se hayan vendido a terceros y fluyan libremente en los mercados de datos. En el contexto de la publicidad conductual, los consumidores no pueden retirar efectivamente su consentimiento cuando lo han proporcionado previamente a las plataformas de gestión del consentimiento,[103] como se ha explicado anteriormente. En la misma línea, cuando los consumidores descargan sus datos de cualquier plataforma,[104] acceden principalmente a los datos que ellos mismos han proporcionado, pero no tienen ni idea de todas las inferencias obtenidas a partir de sus datos ni de a qué categorías de marketing pertenecen en función de esas inferencias, lo que añade una sensación de pérdida de control.

En tercer lugar, los consumidores han ido perdiendo el control sobre sus datos personales debido a las transferencias de datos a terceros países. En la actualidad, más del 90% de los rastreadores contenidos en las aplicaciones móviles son propiedad de empresas con sede en Estados Unidos,[105] y alrededor de 100.000 aplicaciones transfieren datos a más de una jurisdicción, lo que convierte el rastreo por parte de terceros en un fenómeno interjurisdiccional.[106] En la UE, las transferencias de datos a otras jurisdicciones son potencialmente problemáticas para el respeto del derecho fundamental a la intimidad de los ciudadanos de la UE. Esto llevó al TJUE a invalidar la Decisión sobre el Escudo de Privacidad UE-EE. UU. de la Comisión –que permitía la libre circulación de datos entre ambos bloques– en una sentencia de la Gran Sala, con el efecto de prohibir las transferencias de datos de la UE a EE. UU.[107] A pesar de esta sentencia, ¿qué ha pasado con los datos personales que se habían transferido anteriormente? ¿Qué garantías obtendrá la Comisión Europea del gobierno estadounidense en sus negociaciones para un nuevo acuerdo de transferencia de datos? En cualquier caso, este asunto muestra cómo los consumidores pueden perder potencialmente el control de sus datos personales a manos de autoridades extranjeras. Además, el mosaico de normativas relativas a las

[103] VEALE, Michael & ZUIDERVEEN BORGESIUS, Frederik, (2021, de próxima aparición: 25-26).

[104] Hacer uso de su derecho a la portabilidad de los datos según el artículo 20 del RGPD.

[105] La mayoría de los rastreadores pertenecen a Alphabet, Facebook, Twitter, Verizon, Microsoft, LinkedIn y Amazon (BINNS, R. *et al.,* 2018: 27).

[106] BINNS, R. *et al.* (2018: 30).

[107] Sentencia de 16 de julio de 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, EU:C:2020:559.

transferencias transfronterizas de datos parece ser un impedimento para el cumplimiento de los derechos de privacidad y protección de datos de los consumidores.[108]

Por estas razones, parece que el enfoque normativo tradicional sobre el consentimiento, la transparencia y el control ha sido poco adecuado para proteger eficazmente a los consumidores en términos de autonomía y privacidad en la era de la publicidad basada en el comportamiento. Esta conclusión se ve reforzada por la complejidad de la aplicación de sus derechos.

V. UNA APLICACIÓN COMPLEJA Y DÉBIL

En la sección anterior se han destacado muchos de los derechos sustantivos establecidos por el RGPD, que se encuentran entre los más protectores para los consumidores a nivel mundial, a pesar de sus defectos. Sin embargo, estos derechos son aún más ineficaces para protegerlos de la publicidad conductual invasiva si no se aplican adecuadamente. En esta sección se argumenta que la complejidad y la debilidad de la aplicación privada y pública actualmente impiden una protección eficaz de los consumidores. Sin embargo, a pesar de esta observación inicial, esta sección también reconoce los recientes avances positivos en términos de aplicación.

5.1. Aplicación privada

La aplicación privada de los derechos del RGPD no siempre resulta atractiva para los consumidores individuales, ya que las infracciones son difíciles de probar, suelen referirse a reclamaciones de escasa cuantía y los consumidores se enfrentan a actores tecnológicos que disponen de grandes bolsillos para entablar largos litigios.

No obstante, el artículo 80 del RGPD introdujo la posibilidad de que las organizaciones sin ánimo de lucro presentaran reclamaciones ante las autoridades de control, ejercieran el derecho a un recurso judicial efectivo contra las autoridades de control,[109] ejercieran el derecho a un recurso judicial efectivo contra los responsables o encargados del tratamiento,[110] y ejercieran el derecho a recibir una indemnización en nombre de los interesados, cuando así lo dispusiera la legislación de los Estados miembros.[111] Sin embargo, la posibilidad de un recurso colectivo en virtud del RGPD sigue enfrentándose a

---

[108] CASALINI, Francesca, LÓPEZ GONZÁLEZ, Javier & NEMOTO, Taku (2021): "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, https://doi.org/10.1787/ca9f974e-en.

[109] Artículo 78 del RGPD.

[110] Artículo 79 del RGPD.

[111] Artículo 82 del RGPD.

desafíos. En primer lugar, la redacción de la disposición ha sido criticada por ser "bastante confusa",[112] y las resoluciones preliminares del TJUE sobre la posibilidad de dicho recurso colectivo tardarán en materializarse. En segundo lugar, la disposición no obliga a los Estados miembros a prever acciones con exclusión voluntaria ("*opt-out*"), y cuando los Estados miembros la prevén, no hay derecho a compensación.[113] En tercer lugar, cuando los interesados son consumidores, la nueva Directiva sobre acciones representativas deja a los Estados miembros la decisión de si las acciones representativas pueden presentarse en procedimientos judiciales, administrativos o en ambos,[114] lo que podría crear discrepancias entre los Estados miembros. Dicho esto, varias asociaciones utilizaron el artículo 80 para interponer demandas que concluyeron con la imposición de multas récord a los actores de la tecnología publicitaria, como se explica en la siguiente subsección.

5.2. Aplicación pública

La aplicación pública de los derechos del RGPD ha tenido un comienzo lento, y todavía no parece disuadir adecuadamente a las empresas activas en la industria de la tecnología publicitaria de cumplir con el reglamento, principalmente debido a las limitaciones técnicas y a la complejidad del mecanismo de aplicación europeo que creó una aplicación desigual de la ley entre los Estados miembros. No obstante, recientemente han surgido novedades positivas que también se destacarán.

Por un lado, las limitaciones técnicas dificultan a los reguladores el control del cumplimiento de los actores de la tecnología publicitaria. Por ejemplo, el Consejo Noruego del Consumidor señaló la "naturaleza fugaz" de los anuncios, que los hace "muy difíciles de verificar o controlar".[115] Por naturaleza, los anuncios personalizados son diferentes para cada persona, y los reguladores tienen dificultades para controlar el cumplimiento en este contexto. De forma más general, los sistemas de IA (especialmente los que utilizan el aprendizaje profundo, o *"deep learning"*) toman decisiones de forma independiente, esencialmente dentro de una caja negra. De hecho, en los programas de IA "clásicos" en

---

[112] Estudio solicitado por la comisión JURI del Parlamento Europeo, "Collective redress in the Member States of the European Union", octubre de 2018, p. 44, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf [consultado por última vez el 12 de octubre de 2021].

[113] Artículo 80(2) del RGPD.

[114] Considerando 19 de la Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, DO L 409 de 4.12.2020, p. 1-27.

[115] Frobrukerrådet (2021): *Time to Ban Surveillance-Based Advertising: The Case against Commercial Surveillance Online*, https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf, p. 14.

los que las reglas no se aprenden, sino que se codifican con rigor, es el programador humano el que define claramente el proceso de decisión. Por el contrario, como las decisiones basadas en el aprendizaje profundo dependen de los datos utilizados para el aprendizaje (típicamente en cantidades masivas) y el número de parámetros que se calculan en base a estos datos son todos igualmente numerosos (se cuentan en miles de millones de parámetros) se hace imposible hoy en día entender exactamente el razonamiento algorítmico.

Por otra parte, el mecanismo público de aplicación establecido en el RGPD parece estructuralmente defectuoso. Las autoridades nacionales de protección de datos cuentan con amplios poderes de ejecución, aunque las decisiones administrativas nacionales pueden llegar en última instancia al Comité Europeo de Protección de Datos. Dado que algunas de las empresas de tecnología publicitaria más poderosas tienen su establecimiento en la UE en Irlanda (pensemos en Facebook y Google), la DPC (o *"Data Protection Commission"*) irlandesa adquirió un papel destacado en la aplicación de la ley en la UE. Sin embargo, en mayo de 2021, el Parlamento Europeo adoptó una resolución sobre la sentencia *Schrems II* del TJUE,[116] en la que se pide a la Comisión Europea que inicie un procedimiento de infracción contra Irlanda por no aplicar adecuadamente el RGPD.[117] En concreto, los eurodiputados señalan la lentitud en la resolución de los conflictos ante la DPC, que la autoridad no toma medidas proactivas para hacer cumplir el RGPD, que carece de conocimientos técnicos e infraestructuras informáticas, y que intentó sin éxito trasladar los costes de los procedimientos judiciales a la parte demandada. Asimismo, la Comisión abrió un procedimiento de infracción contra Bélgica por la falta de independencia de su APD.[118] Autores también criticaron la falta de rigor en la aplicación de la ley en el sector de la tecnología publicitaria y, en concreto, en el de las ofertas en tiempo real, afirmando que "la situación no es aceptable" y que "crea graves riesgos para el derecho fundamental a la protección de datos en su totalidad".[119]

A pesar de estas conclusiones, los últimos acontecimientos parecen ir en la dirección correcta o, al menos, mitigar los efectos de estos problemas estructurales. En julio de 2021, la APD de Luxemburgo impuso a Amazon una multa récord de 746 millones de euros

---

[116] Sentencia de 16 de julio de 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

[117] European Parliament resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)), P9_TA(2021)0256, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf.

[118] Comisión Europea, Press Release: "June infringements package: key decisions", 9 de junio de 2021, https://ec.europa.eu/commission/presscorner/detail/en/inf_21_2743 [consultado por última vez el 12 de octubre de 2021].

[119] VEALE, Michael & ZUIDERVEEN BORGESIUS, Frederik (2021, de próxima aparición: 37-39).

por violación del RGPD, la mayor multa impuesta a una empresa en virtud del RGPD hasta la fecha. Aunque la empresa hizo pública la multa en una presentación ante la SEC de EE. UU.,[120] que fue confirmada posteriormente por la autoridad,[121] la decisión aún no se ha publicado. No obstante, un comunicado de La Quadrature du Net, que presentó la demanda colectiva contra Amazon, sugiere que la decisión se refiere al sistema de publicidad dirigida de la empresa, ya que la autoridad aparentemente reconoce que no se basa en el libre consentimiento.[122] En septiembre de 2021, la APD irlandesa también impuso una multa de 225 millones de euros a WhatsApp por infringir el principio de transparencia establecido en el artículo 5.1.a del RGPD por no anonimizar los datos personales de los no usuarios, entre otras cosas.[123] Esta última decisión es importante porque demuestra que, aunque la APD irlandesa podría ser reacia a tomar medidas contra las empresas tecnológicas establecidas en Irlanda, el mecanismo de resolución de conflictos entre las APD europeas y la capacidad última del Comité Europeo de Protección de Datos de imponer decisiones vinculantes a las autoridades nacionales pueden dar lugar a importantes sanciones. De hecho, el TJUE sostuvo recientemente en una sentencia de la Gran Sala que, en determinadas condiciones, las APD nacionales pueden llevar cualquier supuesta infracción del RGPD ante el tribunal de un Estado miembro, aunque esa autoridad no sea la APD principal en relación con el tratamiento de datos transfronterizo.[124]

Otras noticias positivas para la aplicación de la ley están relacionadas con la capacidad de los reguladores para supervisar los comportamientos del mercado. Si las empresas utilizan la IA de forma que interfiera en el comportamiento de los consumidores, los reguladores también deberían utilizarla para supervisar el comportamiento de las empresas. Esta es la idea que subyace a la creación por parte del gobierno francés de

---

[120] US Securities and Exchange Commission, Amazon.com, Inc., Form 10-Q, for the quarterly period ended June 30, 2021, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001018724/cbae1abf-eddb-4451-9186-6753b02cc4eb.pdf.

[121] Commission nationale pour la protection des données, « Décision concernant Amazon Europe Core S.à r.l. », August 6, 2021, https://cnpd.public.lu/fr/actualites/international/2021/08/decision-amazon-2.html [consultado por última vez el 12 de octubre de 2021].

[122] La Quadrature du Net, "Amazon fined 746 million euros following our collective action", July 30, 2021, https://www.laquadrature.net/en/2021/07/30/amazon-fined-746-million-euros-following-our-collective-legal-action/ [consultado por última vez el 12 de octubre de 2021].

[123] European Data Protection Board, "EDPB requests that Irish SA amends WhatsApp decision with clarifications on transparency and on the calculation of the amount of the fine due to multiple infringements", 2 de septimebre de 2021, https://edpb.europa.eu/news/news/2021/edpb-requests-irish-sa-amends-whatsapp-decision-clarifications-transparency-and_en [consultado por última vez el 12 de octubre de 2021].

[124] Sentencia de 15 de junio de 2021, *Facebook Ireland Ltd y otros contra Gegevensbeschermingsautoriteit*, C-645/19, ECLI:EU:C:2021:483

PEReN (por *"Pôle d'expertise de la régulation numérique"*),[125] un organismo gubernamental diseñado para apoyar a las autoridades públicas (como la autoridad de protección de datos o la autoridad de la competencia) proporcionando asistencia técnica en los campos del procesamiento de datos, la ciencia de los datos y los procesos algorítmicos para supervisar más eficazmente los algoritmos y las prácticas de las plataformas digitales.[126] De hecho, el PEReN ya está supervisando la adopción de nuevos métodos de seguimiento utilizados por los actores de la tecnología publicitaria, y cree que tendrán un gran impacto en la industria de la publicidad.[127] Si las empresas utilizan la IA para inferir las preferencias de los consumidores, las autoridades deberían utilizarla para inferir cómo funcionan los algoritmos. Esta es la idea que subyace en el método de auditoría de "baja transparencia" de PEReN, que se basa en el análisis estadístico de rastros para inferir los principios de funcionamiento de los algoritmos.[128] Esto permitiría a los reguladores supervisar los algoritmos de caja negra sin ni siquiera la necesidad de acceder al código fuente.

No obstante, estos pocos avances positivos en términos de aplicación no ocultan las principales conclusiones de que los conceptos tradicionales de consentimiento, transparencia y control que se están aplicando lentamente no protegen eficazmente a los consumidores frente a la publicidad basada en el comportamiento. La cuestión de si una aplicación más estricta y coherente será suficiente parece, pues, llevar a un callejón sin salida, si no va acompañada de normas sustantivas más estrictas. De lo contrario, a los consumidores les quedarán poco más que remedios ilusorios de autoayuda, como se explica en la siguiente sección.

VI. LA ILUSIÓN DE LOS REMEDIOS DE AUTOAYUDA

La consecuencia de una aplicación compleja y débil es que los consumidores preocupados por la privacidad tienen que confiar primero en sí mismos si quieren proteger sus datos personales utilizados para la publicidad basada en el comportamiento. Pero los remedios de autoayuda también parecen ineficaces para proteger a los consumidores. Una de las formas más baratas y comunes para que los consumidores se protejan contra

---

[125] Décret n°2020-1102 du 31 août 2020 portant création d'un service à compétence nationale dénommé " Pôle d'expertise de la régulation numérique " (PEReN), *Journal officiel de la République française,* n°0214 du 2 septembre 2020, ELI: https://www.legifrance.gouv.fr/eli/decret/2020/8/31/ECOI2006251D/jo/texte.

[126] INRIA, "Régulation des plates-formes numériques: le gouvernement français prend les devants", 6 mai 2021, https://www.inria.fr/fr/regulation-plateformes-numeriques-peren-regalia.

[127] Véase un resumen de los proyectos de PEReN en: https://www.peren.gouv.fr/projets/.

[128] Véase un resumen de los proyectos de PEReN en: https://www.peren.gouv.fr/projets/.

la publicidad basada en el comportamiento es limitar el rastreo en línea mediante el uso de navegadores web que incorporan tecnologías anti-seguimiento,[129] o extensiones de navegador, por ejemplo. Sin embargo, un estudio reciente muestra que los rastreadores burlan cada vez más estas tecnologías anti-seguimiento.[130] El estudio destaca que estas prácticas dan lugar a un mayor riesgo de fuga de *cookies* a gran escala.[131] También se podría argumentar que esta carrera armamentística en torno a las tecnologías anti-seguimiento es una forma ineficiente de proteger la privacidad de los consumidores. Evidentemente, esta elusión se produce sin ningún tipo de consentimiento, transparencia o control para los consumidores.

Lógicamente, si los consumidores deciden utilizar tecnologías anti-seguimiento para proteger sus datos personales y evitar la elaboración de perfiles con fines de marketing, ¿no debería presumirse que no se da el consentimiento? La evasión de las tecnologías anti-seguimiento parece en sí misma contraria al precepto del RGPD, pero una vez más deja a los consumidores indefensos. En algunos países, las personas que no quieren recibir anuncios en papel en su casa pueden simplemente colocar una pegatina en su buzón de correo indicando que se niega a recibir dichos anuncios (una forma de publicidad mucho menos intrusiva).[132] En línea, el uso de herramientas anti-seguimiento para reducir el riesgo de ser perfilado con fines de marketing infringiendo los derechos fundamentales de los ciudadanos a la intimidad y a la protección de datos no está ni cerca de conseguir el mismo resultado. Y lo que es peor, los consumidores que utilizan tecnologías anti-seguimiento podrían tener comportamientos de navegación que no adoptarían de otro modo, confiando en que no están siendo rastreados, lo que paradójicamente conduce a la divulgación de más datos personales. Por tanto, estas herramientas de autoayuda parecen ser meras ilusiones.

Esto pone de manifiesto la importancia de que los consumidores sepan si están siendo rastreados, o si las condiciones de servicio o las políticas de privacidad de los sitios web que visitan cumplen con el RGPD. Dos iniciativas van en esa dirección. En primer lugar, la asociación de protección de datos NOYB y el Sustainable Computing Lab de la Universidad de Economía y Empresa de Viena están desarrollando una extensión para el

---

[129] Este es el caso de los navegadores Safari y Firefox, pero no el del navegador Chrome de Google (DIMOVA, Yana, ACAR, Gunes, OLEJNIK, Lukasz, JOOSEN, Wouter & VAN GOETHEM Tom (2021): "The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion", in *Proceedings on Privacy Enhancing Technologies*, 3, pp. 394–412. https://doi.org/10.2478/popets-2021-0053).

[130] Ibid.

[131] Ibid, p. 405.

[132] Arrêté du Gouvernement wallon du 23 avril 2020 remplaçant l'arrêt du Gouvernement wallon du 28 février 2019 favorisant la prévention de certains déchets et la propreté publique, *Moniteur belge*, 8 mai 2020, p. 33225.

navegador que enviaría señales automáticas indicando a los sitios web si están consintiendo las *cookies*, lo que permitiría a los consumidores hacer uso de su derecho a oponerse al tratamiento de datos por medios automatizados utilizando las especificaciones técnicas del artículo 21, apartado 5, del RGPD.[133] Esta herramienta de autoayuda también sería más conveniente para los consumidores, ya que no tendrían que lidiar con los banners de *cookies* para cada sitio web que visiten, ya que les permitiría hacer elecciones predeterminadas para todos los sitios web o categorías de ellos. En segundo lugar, el proyecto CLAUDETTE, alojado en el European University Institute, ha desarrollado una herramienta de aprendizaje automático que detecta las cláusulas contractuales abusivas y las violaciones de la legislación sobre protección de datos en las condiciones de servicio o las políticas de privacidad de los sitios web.[134] Estos dos proyectos van en la dirección correcta de dotar a los consumidores de medios técnicos para proteger su privacidad, pero tendrían que ir más allá de la fase de prueba de concepto para ser eficaces.

VII. NECESIDAD DE UNA MAYOR INTERVENCIÓN REGULADORA

Los fallos del mercado y las externalidades producidas por la publicidad conductual y detalladas en las secciones anteriores justifican una mayor intervención reguladora. Regular más estrictamente la publicidad conductual es crucial para proteger la privacidad de los consumidores porque, como modelo principal para financiar los negocios digitales, es omnipresente, y se le ha permitido prosperar durante más de dos décadas. Una mayor regulación de la publicidad conductual también es esencial en la era de la IA, porque las empresas que recogen enormes cantidades de datos personales con fines de marketing también los utilizan para desarrollar potentes herramientas de IA que seguirán dando forma a nuestras sociedades. No es una coincidencia que Google y Facebook no solo sean las mayores empresas de tecnología publicitaria, sino que también estén entre los mayores desarrolladores de IA: tienen acceso a enormes cantidades de datos de comportamiento para alimentar sus algoritmos.

Si el enfoque tradicional en el consentimiento, la transparencia y el control para regular la publicidad basada en el comportamiento no es eficaz para proteger a los consumidores, tal vez la única solución sea una prohibición total. Michael Veale y Frederik Zuiderveen Borgesius sostienen que la propia naturaleza de la publicidad conductual basada en las

---

[133] El proyecto se llama "Advanced Data Protection Control". Véase https://www.dataprotectioncontrol.org.

[134] El proyecto está supervisado por el profesor Hans-W. Micklitz y el profesor Giovanni Sartor en el European University Institute. Véase http://claudette.eui.eu/index.html. Véase también el informe de 2018 del equipo de investigación para la BEUC: "CLAUDETTE meets GDPR Automating the Evaluation of Privacy Policies using Artificial Intelligence", https://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf [consultado por última vez el 12 de octubre de 2021].

pujas en tiempo real la hace incompatible con la legislación europea de protección de datos. Esa es también la conclusión del Consejo Noruego de Consumidores, que pide que se prohíba lo que llama "publicidad basada en la vigilancia", argumentando que la vigilancia comercial generalizada en línea con el fin de mostrar anuncios personalizados a los consumidores no puede justificar las constantes violaciones de los derechos fundamentales.[135]

La adopción de una nueva legislación para regular la publicidad basada en el comportamiento es importante, pero no es la panacea. Por ejemplo, la adopción de un Reglamento sobre privacidad electrónica[136] podría limitar aún más el seguimiento y el uso de patrones oscuros.[137] Del mismo modo, la propuesta de Directiva de Servicios Digitales[138] pretende hacer más transparente la publicidad en línea[139] y los sistemas de recomendación.[140] En su forma actual en el momento de redactar este artículo, también establece un sistema de aplicación de gran alcance, que incluye la concesión a las autoridades de un mayor acceso a los datos de las plataformas muy grandes para un escrutinio adicional.[141] Pero al igual que el RGPD establece protecciones de gran alcance, estas siguen siendo ineficaces si no se aplican correctamente en la práctica.

En ausencia de una aplicación pública de gran alcance, las empresas tecnológicas como Google, Facebook y Apple se presentan a veces como los mayores reguladores de la privacidad.[142] Este argumento está en consonancia con el de Vanessa Mak, según el

---

[135] FROBRUKERRÅDET (2021): *Time to Ban Surveillance-Based Advertising: The Case against Commercial Surveillance Online*, https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf [consultado por última vez el 12 de octubre de 2021].

[136] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017, COM/2017/010 final - 2017/03 (COD).

[137] GRAY, Colin M., SANTOS, Cristiana, BIELOVA, Nataliia, TOTH, Michael, & CLIFFORD, Damian (2021): "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective", in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21), Article 172, pp. 1-18. https://doi.org/10.1145/3411764.3445779.

[138] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15.12.2020, 2020/0361(COD), COM/2020/825 final.

[139] Artículo 29 de la propuesta de DSD.

[140] Artículos 24 y 30 de la propuesta de DSD.

[141] Artículo 31 de la propuesta de DSD.

[142] SCOTT, Mark & MANANCOURT, Vincent, "Google and Apple are the world's biggest privacy regulators", *POLITICO*, 27 de abril de 2021, https://www.politico.eu/article/google-apple-privacy-regulators-gdpr-floc/ [consulto por última vez el 12 de octubre de 2021]; The Economist, "Who should police the web?", 13 de octubre de 2021, https://www.economist.com/leaders/2021/10/13/who-should-police-the-web [consultado por última vez el 13 de octubre de 2021].

cual las plataformas digitales actúan como legisladores privados, en sus ordenamientos jurídicos privados, contribuyendo al pluralismo del derecho privado de la UE.[143] Pero su papel en el mercado no es el de (auto)regular, sino el de proporcionar productos y servicios seguros que respeten los derechos fundamentales de los consumidores. Dado que los contratos de privacidad son muy diferentes de otras categorías de contratos tipo, por las externalidades negativas que generan debido al consentimiento no informado, deberían tratarse con herramientas de regulación de mayor alcance que los conceptos tradicionales de consentimiento y transparencia.[144]

Al mismo tiempo, la cuestión es difícil de abordar porque los principales actores de la tecnología publicitaria tienen un poder de mercado significativo, como demuestran las preocupaciones antimonopolio en el mercado de la publicidad en línea. La posición dominante de Google y Facebook en los mercados de publicidad digital se pone de manifiesto en las decisiones e investigaciones de las autoridades de competencia. En junio de 2021, la Comisión Europea anunció una investigación antimonopolio contra Google en el mercado de la tecnología publicitaria online.[145] Ese mismo mes, la Autoridad Francesa de la Competencia multó a Google con 220 millones de euros por promover sus propios servicios en el sector de la publicidad online.[146] Recientemente, la Comisión abrió una investigación en profundidad sobre la propuesta de adquisición de Kustomer por parte de Facebook, por temor a que ésta tenga una "ventaja de datos" en varios mercados de servicios de publicidad en línea.[147] En EE.UU., Texas está "liderando una coalición multiestatal por múltiples violaciones de las leyes federales y estatales antimonopolio y de protección del consumidor, incluyendo conductas anticompetitivas, prácticas de exclusión y declaraciones engañosas en relación con su papel en el multimillonario sector de la publicidad gráfica en línea". La monopolización de Google de la publicidad gráfica en línea incluye un acuerdo anticompetitivo con Facebook, la realización de declaraciones

---

[143] MAK, Vanessa (2020). *Legal Pluralism in European Contract Law*. Oxford University Press.

[144] En este sentido, véase BEN-SHAHAR, Omri (2019): "Data Pollution", *The Journal of Legal Analysis*, 11, pp. 104-159. https://doi.org/10.1093/jla/laz005.

[145] Comisión Europea, comunicado de prensa: "Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector", 22 de junio de 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3143 [consultado por última vez el 12 de octubre de 2021].

[146] Autorité de la concurrence, "The Autorité de la concurrence hands out a €220 millions fine to Google for favouring its own services in the online advertising sector", 7 de junio de 2021, https://www.autoritedelaconcurrence.fr/en/press-release/autorite-de-la-concurrence-hands-out-eu220-millions-fine-google-favouring-its-own [consultado por última vez el 12 de octubre de 2021].

[147] Comisión Europea, comunicado de prensa: "Fusiones: Commission opens in-depth investigation into proposed acquisition of Kustomer by Facebook", 2 de agosto de 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_4021 [consultado por última vez el 12 de octubre de 2021].

engañosas a los usuarios y clientes, y la supresión de la competencia".[148] A nivel federal en EE. UU., la Federal Trade Commission, con su nueva presidenta Lina Khan, estableció las prioridades de aplicación para la próxima década: las empresas tecnológicas y las plataformas digitales están entre sus objetivos prioritarios.[149]

VIII. CONCLUSIÓN

Este artículo explicó la íntima relación entre la publicidad basada en el comportamiento y la IA, y cómo ese vínculo crea nuevos riesgos para los consumidores en términos de privacidad y autonomía. Estos riesgos son cada vez más omnipresentes, no solo en el mundo digital, sino también en el analógico. Sin embargo, parece que el actual enfoque normativo sobre el consentimiento, la transparencia y el control no ha protegido eficazmente la privacidad y la autonomía de los consumidores. Los reguladores a nivel nacional y de la UE deben seguir interviniendo, de lo contrario los derechos fundamentales de los consumidores a la protección de datos y a la privacidad perderán su esencia y la industria de la tecnología publicitaria seguirá siendo su propio regulador.

En el sector, en la literatura jurídica y entre los reguladores surgen voces para poner fin a la publicidad basada en la vigilancia. Las dificultades para regularla podrían justificar una prohibición total de la publicidad basada en el comportamiento, que parece ser estructuralmente incompatible con los derechos fundamentales de los consumidores a la protección de datos y la privacidad. Si el marco normativo actual, especialmente en el marco del RGPD, permite claramente una aplicación más estricta, nada indica que los actores de la industria de la tecnología publicitaria estén planeando revisar profundamente su modelo de negocio, lo que también queda demostrado por el desarrollo de la cobertura de seguros para los riesgos de ciberseguridad y privacidad.[150] Lo que está claro es que la publicidad puede realizarse de otras maneras, sin la elaboración de perfiles de los consumidores, y que el marketing puede prosperar sin ataques generalizados a la

[148] Fiscal General de Texas, comunicado de prensa: "AG Paxton Leads Multistate Coalition in Lawsuit Against Google for Anticompetitive Practices and Deceptive Misrepresentations", 16 de diciembre de 2020, https://www.texasattorneygeneral.gov/news/releases/ag-paxton-leads-multistate-coalition-lawsuit-against-google-anticompetitive-practices-and-deceptive [consultado por última vez el 12 de octubre de 2021].

[149] Attorney General of Texas, Press Release: “AG Pax-ton Leads Mul-ti-state Coali-tion in Lawsuit Against Google for Anticompetitive Practices and Deceptive Misrepresentations”, December 16, 2020, https://www.texasattorneygeneral.gov/news/releases/ag-paxton-leads-multistate-coalition-lawsuit-against-google-anticompetitive-practices-and-deceptive [consultado por última vez el 12 de octubre de 2021].

[150] OECD (2020), *The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage*. www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf [consultado por última vez el 12 de octubre de 2021].

privacidad y la autonomía de los consumidores. Los reguladores deben asegurarse de que las empresas reciban las señales e incentivos adecuados para hacerlo, pues de lo contrario las leyes de protección del consumidor seguirán pareciendo hipócritas.

IX. BIBLIOGRAFÍA

ACAR, Gunes, JUAREZ, Marc, NIKIFORAKIS, Nick *et al*. (2013). "FPDetective: Dusting the Web for Fingerprinters", in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 1129–1140. https://doi.org/10.1145/2508859.2516674.

ACQUISTI, Alessandro, TAYLOR, Curtis & WAGMAN, Liad (2016): "The Economics of Privacy", *Journal of Economic Literature*, 54(2), pp. 442-492. http://dx.doi.org/10.1257/jel.54.2.442.

AGGARWAL, Nikita (2021): "The Norms of Algorithmic Credit Scoring", *The Cambridge Law Journal*, 80(1), pp. 42-73. https://doi.org/10.1017/S0008197321000015.

ANDRÉ, Quentin, CARMON, Ziv, WERTENBROCH, Klaus *et al*. (2018): "Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data", *Customer Needs and Solutions*, 5, pp. 28–37. https://doi.org/10.1007/s40547-017-0085-8.

ANNANY, Mike & CRAWFORD, Kate (2016): "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability", *New Media & Society*, 20(3), pp. 973-989. https://doi.org/10.1177%2F1461444816676645.

BAKOS, Yannis, MAROTTA-WURGLER, Florencia & TROSSEN, David (2014): "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts", *The Journal of Legal Studies*, 43(1), pp. 1–35.

BEN-SHAHAR, Omri (2019): "Data Pollution", *The Journal of Legal Analysis*, 11, pp. 104-159. https://doi.org/10.1093/jla/laz005.

BEN-SHAHAR, Omri & PORAT, Ariel (2021): *Personalized Law*, Oxford University Press.

BEN-SHAHAR, Omri & SCHNEIDER, Carl E. (2014). More Than You Wanted to Know: The Failure of Mandated Disclosure. Princeton University Press.

BEN-SHAHAR, Omri & STRAHILEVITZ, Lior (2016): "Contracting Over Privacy: Introduction", *Journal of Legal Studies*, 45(2), pp. 1-11.

BINNS, R. *et al.* (2018): "Third Party Tracking in the Mobile Ecosystem", in *Proceedings of the 10th ACM Conference on Web Science*, pp. 23-31. https://doi.org/10.1145/3201064.3201089.

BUSCH, Christoph (2019): "Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law", *The University of Chicago Law Review*, 86, pp. 309-331.

CASALINI, Francesca, LÓPEZ GONZÁLEZ, Javier & NEMOTO, Taku (2021): "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, https://doi.org/10.1787/ca9f974e-en.

CMA (2020) "Online Platforms and Digital Advertising: Market Study Final Report," pp. 1–437. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

COFONE, Ignacio & ROBERTSON, Adriana (2018): "Consumer Privacy in a Behavioral World", *Hastings Law Journal*, 69(6), pp. 1471-1508. https://repository.uchastings.edu/hastings_law_journal/vol69/iss6/1.

DE MONTJOYE, Yves-Alexandre, RADAELLI, Laura, KUMAR SINGH, Vivek & PENTLAND, Alex 'Sandy' (2015): "Unique in the shopping mall: On the reidentifiability of credit card metadata", *Science*, 347(6221), pp. 536-539. https://doi.org/10.1126/science.1256297.

DE MONTJOYE, Yves-Alexandre, HIDALGO, César, VERLEYSEN, Michel & BLONDEL, Vincent (2013): "Unique in the Crowd: The Privacy Bounds of Human Mobility", *Scientific Reports*, 3: 1376. https://doi.org/10.1038/srep01376.

DIMOVA, Yana, ACAR, Gunes, OLEJNIK, Lukasz, JOOSEN, Wouter & VAN GOETHEM Tom (2021): "The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion", in *Proceedings on Privacy Enhancing Technologies*, 3, pp. 394–412. https://doi.org/10.2478/popets-2021-0053.

EDWARDS, Lilian & VEALE, Michael (2017): "Slave to the Algorithm", *Duke Law and Technology Review*, 16(1), pp. 18-84.

ENGLEHARDT, Steven & NARAYANAN, Arvind (2016): "Online tracking: A 1-million-site measurement and analysis", in *CCS 2016 - Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1388-1401. https://doi.org/10.1145/2976749.2978313.

FARZANEHFAR, Ali, HOUSSIAU, Florimond & DE MONTJOYE, Yves-Alexandre (2021): "The risk of re-identification remains high even in country-scale location datasets", Patterns, 2(3): 100204, https://doi.org/10.1016/j.patter.2021.100204.

FROBRUKERRÅDET (2021): *Time to Ban Surveillance-Based Advertising: The Case against Commercial Surveillance Online*. https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf.

FROBRUKERRÅDET (2018). *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

GRAY, Colin M., SANTOS, Cristiana, BIELOVA, Nataliia, TOTH, Michael, & CLIFFORD, Damian (2021): "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective", in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*, Article 172, pp. 1-18. https://doi.org/10.1145/3411764.3445779.

GRUSON, Damien, HELLEPUTTE, Thibault, ROUSSEAU, Patrick & GRUSON, David (2019) "Data science, artificial intelligence, and machine learning: Opportunities for laboratory medicine and the value of positive regulation", *Clinical Biochemistry*, 69, pp. 1-7. https://doi.org/10.1016/j.clinbiochem.2019.04.013

KOROBKIN, Russell (2003): "Bounded Rationality, Standard Form Contracts, and Unconscionability", *University of Chicago Law Review*, 70(4), pp. 1203-1295.

KRAMER, Adam, GUILLORY, Jamie & HANCOCK, Jeffrey (2014): "Experimental evidence of massive-scale emotional contagion through social networks", in *Proceedings of the National Academy of Sciences*, 111(24), pp. 8788-8790; https://doi.org/10.1073/pnas.1320040111.

MAK, Vanessa (2020). *Legal Pluralism in European Contract Law*. Oxford University Press.

MAROTTA-WURGLER, Florencia (2011): "Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's 'Principles of the Law of Software Contracts'", *University of Chicago Law Review*, 78(1), pp. 165-186.

MARTINI, Mario (2020): "Regulating Algorithms: How to Demystify the Alchemy of Code?" in EBERS, Martin & NAVAS, Susana (Eds.), *Algorithms and Law* (pp. 100-135), Cambridge University Press. https://doi.org/10.1017/9781108347846.004.

MATHUR, Arunesh *et al.* (2019): "Dark patterns at scale: Findings from a crawl of 11K shopping websites", in *Proceedings of the ACM on human-computer interaction*, 3(CSCW), pp. 1–32. https://doi.org/10.1145/3359183.

MIK, Eliza (2016): "The Erosion of Autonomy in Online Consumer Transactions", *Law, Innovation and Technology*, 8(1), pp. 1-38. https://doi.org/10.1080/17579961.2016.1161893.

NORBERG, Patricia, HORNE, Daniel, & HORNE, David (2007): "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *Journal of Consumer Affairs*, 41(1), pp. 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x.

NOUWENS, Midas, LICCARDI, Ilaria, VEALE, Michael, KARGER, David & KAGAL, Lalana (2020): "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery*, pp. 1–13. https://doi.org/10.1145/3313831.3376321.

ROCHER, Luc, HENDRICKX, Julien M. & DE MONTJOYE, Yves-Alexandre (2019): "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature Communications,* 10(3069), https://doi.org/10.1038/s41467-019-10933-3.

SCHNEIDER, Carl E. & BEN-SHAHAR, Omri (2010): "The Failure of Mandated Disclosure", John M. Olin Program in Law and Economics Working Paper No. 516, https://chicagounbound.uchicago.edu/law_and_economics/520/.

VEALE, Michael & ZUIDERVEEN BORGESIUS, Frederik, (2021, forthcoming): "Adtech and Real-Time Bidding under European Data Protection Law", *German Law Journal*. https://doi.org/10.31235/osf.io/wg8fq.

VÉLIZ, Carissa (2021): *Privacy is Power*, London: Bantam Press.

WACHTER, Sandra & MITTELSTADT, Brent (2019): "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, 2019(2), pp. 1-130.

WAGNER, Ben, WINKLER, Till & HUMAN, Soheil (2021): "Bias in Geographic Information Systems: The Case of Google Maps," in *Proceedings of the 54th Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences. https://epub.wu.ac.at/id/eprint/7801.

ZUBOFF, Shoshana (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile Books.

TOWARDS THE DEHUMANIZATION OF THE CONTRACT FORMATION PHASE. ALGORITHMIC CONTRACTING AND SMART CONTRACTS

Por

MARIA L MENA
Lawyer. PhD Researcher King's College London

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

ABSTRACT: Smart contracts, originally introduced in the 1990s by Nick Szabo, have gained prominence with the rise of blockchain technology, and with the latest developments in algorithmic contracting. Their impact on contract law is evident, and therefore this paper analyzes from the English contract law perspective their formation phase in order to become legally enforceable. In addition, the analysis is carried out separately with respect to smart contracts whose formation phase is prior to their translation into code, from those in which algorithms are involved in the contract formation phase, which presents greater complexities. The purpose of this paper is to highlight the challenges presented by the legal framework of smart contracts in order to prepare the basis for future research on ways to address these concerns.

KEYWORDS: smart contracts, contract formation, algorithmic contracts.

SUMMARY: I. INTRODUCTION. II. CONTRACT'STAGES: THE FORMATION OF SMART CONTRACTS. 1. Offer and acceptance. 2. Intention. 3. Consideration. 4. Vitiating factors. 4.1. Vitiating factors enabled by smart contracts' anonymity. 4.2. Vitiating factors enabled by code. 4.3. An initial thought on how to overcome vitiating factors. III. DEHUMANIZING THE CONTRACT FORMATION PHASE IN SMART CONTRACTS: ALGORITHMIC SMART CONTRACTS. IV. CONTRACTUAL FREEDOM AND CONTRACT FORMALITIES: LANGUAGE AND SIGNATURE. V. CONCLUSIONS.

HACIA LA DESHUMANIZACIÓN DE LA FASE DE FORMACIÓN DEL CONTRATO. CONTRATACIÓN ALGORÍTMICA Y CONTRATOS INTELIGENTES

RESUMEN: Los contratos inteligentes, introducidos originalmente en la década de 1990 por Nick Szabo, han ganado protagonismo con el auge de la tecnología blockchain, y con los últimos desarrollos en materia de contratación algorítmica. Su impacto en el derecho contractual es evidente, por lo que este trabajo analiza desde la perspectiva del derecho contractual inglés su fase de formación para llegar a ser legalmente exigibles. Además, el análisis se realiza de forma separada respecto a los contratos inteligentes cuya fase de formación es previa a su plasmación en código, de aquellos en los que los algoritmos intervienen en la fase de formación del contrato, lo que presenta mayores complejidades. El objetivo de este trabajo es poner de manifiesto los retos que presenta el marco jurídico de los contratos inteligentes con el fin de preparar las bases para futuras investigaciones sobre las formas de abordar estas preocupaciones.

PALABRAS CLAVE: contratos inteligentes, formación de contratos, contratos algorítmicos.

I. INTRODUCTION

Szabo defined Smart Contracts for the first time in 1994 as "a computerized transaction protocol that executes the terms of a contract".[1] His original idea was meant to develop a digital institution taking advantage from the tradition of "our current laws, procedures, and theories" using algorithms and cryptography to replace traditional business relationships moving them to the cyberspace.[2] Szabo specifically pointed out that "[t]he idea behind smart contracts is that many kids of contractual clauses (such collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher".[3] But Szabo's ideas require in-depth analysis not only for what he said, but because ultimately, "contracts and contract law can, and indeed often do, have a formally logical structure" similar to computational logic,[4] and as a consequence a movement towards automation has been developing over the last few decades. This tendency has reached greater heights of interest as a consequence of the implementation of blockchain technology in smart contracts.

Throughout the literature on smart contracts, terms such as agreement, contract, promises, transactions, are sometimes used without legal rigor. Leaving aside the concept of smart contract as code, the aim of this paper is analyzing how "legal contracts can be expressed and implemented in software",[5] not only because this was the indented purpose of its coiner, but also because, although not unanimously accepted, it is said that "smart contracts should nonetheless be considered contracts because they are agent-generated mechanisms to shift rights and obligations".[6]

This paper is divided in four sections. Section 2 discusses the formation stage of smart contracts, analyzing the possible concurrence in smart contracts of each doctrinal

---

[1] Nick Szabo, 'Smart Contracts' <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.

[2] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' 2 <https://search.datacite.org/works/10.5210/fm.v2i9.548>.

[3] Ibid

[4] Jeffrey M Lipshaw, 'The Persistence of "Dumb" Contracts' (2019) 2.1 1, 30 <https://stanford-jblp.pubpub.org/pub/persistence-dumb-contracts/release/1>.

[5] Christopher D Clack, Vikram A Bakshi and Lee Braine, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' <https://arxiv.org/abs/1608.00771>.

[6] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 126 <https://papers.ssrn.com/abstract=2936294> accessed 24 September 2020.

requirement for a contract to be legally enforceable. In relation to those requirements also analyzes contracts' vitiating factors. Section 3 moves beyond mixed-analog smart contracts and analyzes such requirements form a perspective of algorithmically formed smart contracts. Section 4 considers the principle of freedom of contract from the point of view of smart contracts, as well as the impact of code language and cryptographic signature with respect to certain contractual formalities. And Section 5 concludes.

II. CONTRACT' STAGES: THE FORMATION OF SMART CONTRACTS

There are many definitions of contract, depending on sources and jurisdictions, but I am going to consider in this paper English contract law, to approach smart contracts legality from a common law perspective. "A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some ways recognizes as a duty".[7] But it should be also noticed that "[t]he term 'contract' refers both to the agreement and to its embodiment".[8] In general terms this embodiment can be written, but also spoke or coded. And despite the term being used interchangeably, the source of rights and obligations is the agreement itself, no its embodiment. If, as stated by Cartwright, "the aim of the law of contract is to facilitate the parties' own creation of legally enforceable obligations",[9] and as Szabo pointed out "[t]he contractual phases of search, negotiation, commitment, performance, and adjudication constitutes the realm of smart contracts",[10] there are reasons to believe that contract law might as well support the so-called Smart Legal Contracts.[11] To prove this statement, "self-updating properties"[12] of contract law will be under scrutiny in this section.

The requirements for contract formation are not excessively different from one jurisdiction to another, but for the aim of this paper I will refer to English contract law because common law has traditionally proved to be more flexible to adaptations and

---

[7] Burrows FBA Andrew QC (Hon), Sir Jack Beatson FBA and John Cartwright, *Anson's Law of Contract* (Oxford University Press 2016) 2 <http://dx.doi.org/10.1093/he/9780198734789.001.0001>.

[8] Eliza Mik, *The Resilience of Contract Law in Light of Technological Change* (Michael Furmston ed, 2020) 112 13.

[9] John Cartwright, *Contract Law* (Hart Publishing 2016) 98 <http://bvbr.bib-bvb.de:8991/F?func=service&doc_library=BVB01&local_base=BVB01&doc_number=029010258&sequence=000001&line_number=0001&func_code=DB_RECORDS&service_type=MEDIA>.

[10] Szabo, Formalizing and Securing Relationships on Public Networks (n …)

[11] "[A] Smart Legal Contract is a legal contract that becomes smart, it's legal by design and thanks to the right tools, can implement a smart component". See Glauco Ciprari, ' #Blockchainn & #Smart Legal Contracts. Make Smart a #LegalContract - Approach Models and Hands On' (Bocconi University 2021).

[12] Mik, *The Resilience of Contract Law in Light of Technological Change* 112.

generally more business focused. Therefore presumably it will be easier to find the legal fit of smart contracts which will respond more effectively to the use of this new technology in commercial transactions.[13]

But, "[d]oes contract law do what smart contracts aim to do?".[14] I argue that they are two different things. Contract law is the framework, and smart contracts are means by which the meeting of the minds is captured and set out, but also, and this is the novelty, are the means by which this meeting of the minds is executed, preventing the contracting parties from a voluntarily breach. Some argue that a new law, a Lex Cryptographia, will emerge "as rules administered through self-executing smart contracts and decentralized organizations".[15]

Not every smart contract is a contract. "[A] Smart Legal Contract is a legal contract that becomes smart, it's legal by design and thanks to the right tools, can implement a smart component".[16] A smart legal contract is made up pieces of smart contract code.[17] In order to analyze how smart contracts might fit within contract law's boundaries to become legal by design, the life of a contract has to be carefully scrutinized and compared in both an analogic and a smart contract, and doctrinal reconciliation is required. However, and therein lies the novelty, it is important to consider that, as Eliza Mik points out "[c]ontractual relationships have never been regulated on the basis if the technology used to facilitate the process of contract formation and/or performance".[18]

Although on smart contracts collapse "the distinction between agreement formation and execution",[19] the analysis of the contract formation phase will be the subject of this paper, for comparative purposes with traditional contracts. Because "an agreement is more than a coincidence of intentions",[20] for the aim of this analysis we are going to consider that the formation of a contract covers from the agreement itself, intention, and consideration, and in doing so this section will approach also the vitiating factors.

---

[13] For a more in-depth analysis of the superior effectiveness of common law as opposed to civil law see Nuno Garoupa and Carlos Gomez Liguerre, 'The Syndrome of the Efficiency of the Common Law' (2011) 29 287, 287.

[14] Werbach and Cornell 141.

[15] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' 1. See also Werbach and Cornell 313, 319.

[16] Ciprari.

[17] 'Smart Contracts And Distributed Ledger - A Legal Perspective' (2017) <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>.

[18] Mik, *The Resilience of Contract Law in Light of Technological Change* 112.

[19] Jeremy M Sklaroff, 'Smart Contracts and the Cost of Inflexibility ' (2017) 166 263, 276 <https://www.jstor.org/stable/45154933>.

[20] Cartwright 95.

There is a general agreement that smart contracts' formation stage can adjust to contract law principles.[21] There is no doubt that this happens in the case of 'mixed analog-smart legal contracts', in which once the contract has been agreed, it is translated into code. In those the formation phase is completed as an analog traditional contract, and only the execution remains smart. But having said that, some nuances have to be carefully considered too. Those, concluded and executed, smart contracts will be covered separately in the following section.

1. Offer and acceptance

A legal formal definition of offer can be found in Anson's Law of Contracts:

> "An offer is an intimation, by words or conduct, of a willingness to enter into a legally binding contract, and which is in its terms expressly or impliedly indicates that it is to become binding on the offeror as soon as it has been accepted by an act, forbearance, or return promise on the part of the person to whom it is addressed".[22]

Formation of a contract requires an offer by one party and an acceptance by the other, and an objectivity theory applies in order to ascertain the existence of the agreement. "[A] consensus ad idem -'a meeting of the minds' is required for the contract to be formed".[23] Nothing changes in relation to the offer and acceptance dynamics when we refer to what I have called before as 'mixed analog-smart legal contracts', because the formation stage takes place off-line and then is translated into code. If the insinuation by conduct can be qualified as a valid offer, I agree with Filatova when she says that "deployment of a smart contract on blockchain may qualify as an offer".[24] This scenario represents, however, a step further compared to mixed-analog legal smart contracts, as there is no prior offline negotiation as referred to above.

Hence, things are differently when the initial offer is already coded, and blockchain technology is used to enable contact between the contracting parties. "[A]n acceptance is

---

[21] Mateja Durovic and André Janssen, *Formation of Smart Contracts under Contract Law* (Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò eds, Cambridge University Press 2019) 61 10 <https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/formation-of-smart-contracts-under-contract-law/5935C0C4FE5AB265B25697D8107D8D25> accessed 2020. Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 305, 322.

[22] Andrew, Beatson FBA and Cartwright 35.

[23] Durovic and Janssen 12.

[24] Nataliia Filatova, 'Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies' (2020) 28 217, 225 <https://academic.oup.com/ijlit/article/28/3/217/5897086> accessed 13 October 2020.

the offeree's unequivocal assent to the offer with a view to concluding the contract".[25] It can be expressed not only by formal means such as a signature or using a cryptographic key, but also by performance pursuant to the terms of the agreement. In any case "there is a clear act of acceptance".[26] An offer in contract law infers an intent to be bound, and that requirement distinguishes an offer from a mere invitation to treat. In smart contracts the deployment of an offer on the blockchain implies, rather than infers, that intent, and thus turns it in a kind of 'suspensive' offer.

There is a general agreement around the fact that contract law rules of offer and acceptance fit for governing smart contracts.[27] "Deploying a smart contract to a distributed ledger and signing the smart contract with a private key should constitute a valid offer and acceptance".[28] Raskin argues that in smart contracts "acceptance comes through performance".[29] In my opinion, on the contrary, unstoppable performance comes through acceptance. Signing a smart contract is the external evidence that a consensus has been reached between the offeror and the offeree, and this, automatically and irreversibly, sets in motion the execution of the agreement, and no revocation of the offer or the acceptance is possible.

When the initial offer is already encrypted, smart contracts become a new kind of standard form contracts, because the terms of the contract are largely imposed by one of the parties. The use of standard form contracts became widespread with the advent of e-commerce, and so we look back to e-commerce when analyzing the concurrence of mutual assent in smart contracts. 'Clickwrap' or 'browse-wrap' solutions and the way in which these solutions make the terms accessible to the contracting parties have been under scrutiny in order to have a place in e-commerce in defense of consumers,[30] but in the case of smart contracts it is different because this would imply the mandatory existence of a written part in natural language accessible to the parties and not purely code.[31] Moreover, smart contracts differ from standard form contracts in the fact that, as

[25] Cartwright 114.

[26] Durovic and Janssen 11.

[27] See ibid 10. and Werbach and Cornell.

[28] 'Smart Contracts: Is The Law Ready?' (2018) 14 <https://digitalchamber.s3.amazonaws.com/Smart-Contracts-Whitepaper-WEB.pdf>.

[29] Raskin 322.

[30] Reggie O'Shields, 'Smart Contracts: Legal Agreements for the Blockchain' (2017) 21 177, 186. For a brief analysis of the so-called click and browse-wrap agreements in e-commerce, see also Mik, *The Resilience of Contract Law in Light of Technological Change* 21-2.

[31] One of the main differences between e-commerce and smart contracts is that the former are written in natural language and the later are written in code. See Sai Agnikhotram and Antonios Kouroutakis, 'Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, "Smart" Way to Contract? ' 300, 315.

soon as it is deployed on the blockchain, it becomes binding for the offeror because if it is accepted it will be executed automatically and irreversibly.

Time and place of acceptance and their specificities have been developed through time by courts, and the general rule is that there is no contract until the acceptance has arrived, due to delays in communication. The 'postal rule' has evolved with the rise of new technologies. In smart contracts, acceptance can occur simultaneously with offer if there is any sort of-line pre-smart contract bargain, or after the offer is coded on the smart contract and reaches the other party, but in both cases, once accepted, is triggered and the offeror cannot step back. It is to consider that smart contracts are released on the blockchain, and "blocks on Ethereum are committed approximately once every fifteen seconds".[32] At this stage, it is not yet possible to state categorically that some variation of the postal rule will not need to be applied to smart contracts.

2. Intention

As Anson's Law of Contracts states "an agreement will not constitute a binding contract unless it is one which can reasonably be regarded as having been made in contemplation of legal consequences".[33] Under English contract law, intention to create legal relations is generally presumed by the concurrence of two elements, namely "the fact of the agreement and the existence of consideration".[34] Intention must be manifested or communicated,[35] and intention is tested objectively.[36] In relation to smart contracts some argue that "[t]he fact that that parties submit their cryptographic private keys to commit their resources to the smart contract is proof of such an intent",[37] and therefore being manifested, communicated and objectively verifiable, a preliminary conclusion would be that the intent requirement is present in smart contracts. However, although it may seem obvious, it is important to point out that contract law refers to the "intention to create legal relationships".[38]

A different point of view can be found in Savelyev's approach to smart contracts. He considers smart contracts as an alternative to contract law and in doing so, he suggests

[32] 'Blocks' <https://ethereum.org> accessed 11 March 2021.

[33] Andrew, Beatson FBA and Cartwright 73-4.

[34] Cartwright 156.

[35] Mik, *The Resilience of Contract Law in Light of Technological Change* 112.

[36] Andrew, Beatson FBA and Cartwright 34.

[37] Werbach and Cornell 156.

[38] Andrew, Beatson FBA and Cartwright 73.

that the intention of the parties might not be "to create legal relations".[39] He argues though that the parties to a smart contract have "an intention to use alternative regulatory system, not a classic contract law".[40] Leaving apart libertarian utopianism discussions, intention means the same in Savelyev's smart contracts idea and in traditional contract law: to be bound by a consequence.

Hence at a very first sight the requirement of intent can be found on smart contracts, by means of representing their obligations in code.[41] An additional concern about intention is pointed out also by Mik. She highlighted that although it might be no doubt about the parties' intention to be contractually bound, problems may arise when implementation does not match intention,[42] which would place us in the field of vitiating factors, which will be analyzed later in this section.

3. Consideration

"A valuable consideration, in the sense of the law, may consist in some right, interest, profit, or benefit accruing to the one party, or same forbearance, detriment, loss or responsibility given, suffered, or undertaken by the other",[43] and therefore "[s]mart contracts would be contracts as long as they meant to alter concretely the normative relation between the parties".[44] Also, consideration "need not be adequate but it must be of some value in the eye of the law".[45] Although some scholars flatly assert that there is consideration in smart contracts,[46] there is no unanimity and therefore the question that arises is how this legal requirement may fit on smart contracts. In fact, we can reduce the number of smart contracts that can be smart legal contracts if we start from the premise that "only those smart contracts that involve exchanges can fulfill the requirement of consideration".[47]

---

[39] Alexander Savelyev, 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law' (2016) 11 <https://papers.ssrn.com/abstract=2885241> accessed 24 September 2020.

[40] ibid.

[41] Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9 269, 15 <http://www.tandfonline.com/doi/abs/10.1080/17579961.2017.1378468>.

[42] ibid 11.

[43] Currie v Misa [1875] LR 10 Ex 153, [162]

[44] Werbach and Cornell 128.

[45] Andrew, Beatson FBA and Cartwright 104.

[46] Raskin 322.

[47] Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' 14.

Problems with consideration is one of the 'Doctrinal Concerns' pointed out by Werbach and Cornell in relation to smart contracts.[48] "For smart contracts, there is no test for consideration", they argue.[49] Posting a smart contract on the blockchain "does not commit any party to do anything".[50] According to them, there is no consideration because instead of something being executed in the future in the event that something happens, it is the technology that will make it happen. Similarly Eliza Mik argues that the most generalized use of smart contracts is being "unilateral transfer mechanisms: software programs enabling the automated generation or transfer of crypto-assets upon the occurrence of pre-defined conditions".[51] Unilateral is quite the opposite of an exchange.

However, in my opinion, what happens is that the execution is not of the commitment itself, but the means to automatically execute that commitment in an irreversible way, and this constitutes the consideration in smart contracts. The promise to pay or to perform is fulfilled simultaneously because it is irrevocable, "collapsing the distinction between agreement formation and execution".[52] The fact that the performance do not depend on the debtor's acts does not mean that there is no obligation.[53] As De Caria states, "by entering into a smart contract, parties undertake to perform the obligation therein encapsulated".[54] Savelvey explains this from a different approach by saying "the main consequence of conclusion of Smart contract is not an appearance of 'obligations' but the resulting self-limitation of certain rights by technical means".[55] This self-limitation equals to pay or perform in the future in the case of traditional analogic contracts.

A more complex situation is whether smart contracts fit when a non-performance obligation is involved, since a priori smart contracts aim at automatic performance, performance being precisely a term opposed to inactivity or non-performance. This could be situations in which the smart contract executes the guarantee offered in the event of non-performance of the obligation not to do. This would be the use of the smart contract as escrow.[56]

---

[48] Werbach and Cornell 155-162.

[49] ibid 158.

[50] Ibid 129.

[51] Mik, *The Resilience of Contract Law in Light of Technological Change* 14.

[52] Sklaroff 276.

[53] Filatova 225.

[54] Riccardo De Caria, 'The Legal Meaning of Smart Contracts' (2018) 26 731, 747 <http://www.kluwerlawonline.com/abstract.php?area=Journals&id=ERPL2018052>.

[55] Savelyev 18.

[56] See Werbach and Cornell 132-3. (analyzing the potential of smart contracts to be employed in the implementation of deposit agreements, differentiating them from their consideration as a escrow per se.)

Werbach and Cornell also argue that there is no consideration in smart contracts by means of an inverse logical deduction. They state that some smart contracts could serve to encode promises or agreements that cannot be considered contracts under the contract law and therefore cannot be enforced. And because there is no consideration on those, there is no consideration in smart contracts. On the contrary, Savelyev points out that smart contracts will not be used in situations in which analogic contracts are normally made such as social invitations.[57] Whether they are used or not for that purpose, that circumstance does not turn a smart contract into a smart legal contract.

Another requirements to analyze in relation with consideration is that "[c]onsideration must be real",[58] but digital assets such as tokens or cryptocurrencies do not physically exist. They are virtual ledger entries, that might represent real assets or rights in the off-line word or just exist virtually. A first sight their legal status was controversial, and has been subject of analysis.[59] But the pieces have finally fit into the puzzle and the UK Jurisdiction Taskforce in its report "Legal statement on cryptoassets and smart contracts",[60] concluded that cryptoassets can be treated as property, which ultimately has been ratified by the English Court ruling that "cryptoassets such as Bitcoin are property".[61]

Consideration can concur in smart contracts, and those fulfil contract law's requirements and, therefore, can be considered as smart legal contracts. In the same way that as pointed out before, "[t]he term 'contract' refers both to the agreement and to its embodiment",[62] consideration is "essential both to the form and the substance of a contract".[63] Ultimately what distinguishes smart contracts as 'pieces of software'[64] or 'technical artifacts',[65] from smart legal contracts, is that smart contracts that are legal by design.

---

[57] Savelyev 11.

[58] Andrew, Beatson FBA and Cartwright 106.

[59] See Kelvin FK Low and Ernie GS Teo, 'Bitcoins and Other Cryptocurrencies as Property?' (2017) 9 235, 235-268 <https://doi.org/10.1080/17579961.2017.1377915> accessed 15 March 2021.

[60] 'Legal Statement on Cryptoassets and Smart Contracts' (2019) <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf>.

[61] AA v Persons Unknown [2019] EWHC 3556 (Comm)

[62] Mik, *The Resilience of Contract Law in Light of Technological Change* 13.

[63] Andrew, Beatson FBA and Cartwright 136.

[64] Caria 739.

[65] Karen Levy refers to smart contracts as 'technical artifacts' when they are considered as mere code, leaving aside relational contexts. See Karen EC Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law' (2017) 3 1, 2

4. Vitiating factors

"Not all the factors that vitiate a contract are uniform in effect. Some of them may render a contract void or illegal, others voidable, while others still may make the contract unenforceable at the suit of one or other of the parties. These terms (void, illegal, voidable, and unenforceable) therefore denote different degrees of ineffectiveness".[66]

For Werbach and Cornell "[t]he distinctive aspect of smart contracts is not that they make enforcement easier, it is that they make enforcement unavoidable".[67] In my opinion, it is not a matter of enforcement, but of immutable and tamper proof execution, but the occurrence of vitiating factors cannot be excluded in smart contracts, and therefore how this factors can affect the formation of smart contracts should not be underestimated. Ultimately, "[t]he usual defenses to formation of a contract also apply in the realm of smart contracts".[68]

As introduced above, the formation of a contract requires the exchange of the parties' consents, and although the objective test is applied in contract law, a smart contract, as any contract, might be vitiated by mistake, misrepresentation, non-disclosure, duress, undue influence or by being an unconscionable bargain.[69] They can be categorized as defenses to contract formation, such as mistake, misrepresentation, frustration, unconscionability, and satisfaction, and defenses against formation, such as lack of capacity or duress. However, there is no doctrinal analysis around the specificities of smart contracts' vitiating factors, their potential consequences and possible ways to deal with them, other than a few brief mentions through the literature.[70] Hence, to approach them, instead of using the traditional classification I have referred to above, defenses to contract formation and defenses against formation, I will refer to vitiating factors in terms of their enabling factor in smart contracts, namely anonymity and code.

4.1. *Vitiating factors enabled by smart contracts' anonymity*

<https://explore.openaire.eu/search/publication?articleId=doajarticles::3e00f2f81bb4e4541367a8900c053957>..

[66] Andrew, Beatson FBA and Cartwright 23-4.

[67] Werbach and Cornell 136.

[68] Raskin 325.

[69] Cartwright 159.

[70] See e.g. Werbach and Cornell 371. Pierluigi Cuccuru, 'Beyond Bitcoin: An Early Overview on Smart Contracts' (2017) 25 179, 191 <https://academic.oup.com/ijlit/article/25/3/179/3106217> accessed 16 November 2020.; Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen, 'Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts' (2019) 35 69, 16 <https://search.datacite.org/works/10.1016/j.clsr.2018.09.003>.

The fact that a contractual relationship can be initiated under duress or by mistake is a fact that can occur both online and in the analog world, both in a traditional analogic contract and in a smart contract. However, in relation to these vitiating factors, there are some differences between traditional contracts and smart contracts that can be particularly challenging due to the pseudo-anonymity of smart contracts. Smart contracts built on blockchain platforms are "asymmetrically encrypted",[71] what means that it has a two-steps verification system which in practice involves that each user holds both, a public and a private key, mathematically related "by virtue of which the private key can decrypt data that has been encrypted through the public key".[72] The public key is the one that, shared with another user, enables the transaction, and because additional data is required to identify the person behind it, it is consider pseudonymous data.

"In most contracts the identity of the other party is not significant",[73] and in this sense anonymity is not an additional threat in smart contracts.[74] But still, mistakes about identity of the other party can concur and are relevant if the identity of the party to the contract is a fundamental aspect to enter into the agreement. Filatova distinguishes three situations in relation with the identification of the parties: first, if a smart contract is a part of a traditional contract, contracting parties would have communicated previously off-chain, and therefore identification is not an issue; second, if a smart contract is a contract *per se*, pseudo-anonymity, as pointed out before, is not an obstacle itself, and problems may arise only in case of malfunction; and third, if a smart contracts is a facilitator for contract performance, there is no problem because only affects to contract performance and not to its formation stage.[75]

But not only does the identity not refer exclusively to the name of the specific person or the company name of the specific commercial company, as in traditional contracts, but in smart contracts it also refers to the specific link between the cryptographic signature

---

[71] Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers Reports: Practitioner's Corner' (2016) 2 422, 422 <https://heinonline.org/HOL/P?h=hein.journals/edpl2&i=448> accessed 9 December 2020.

[72] Michèle Finck, 'Blockchain and the General Data Protection Regulation' (EPRS European Parliamentary Research Service 2019) 26 <http://publications.europa.eu/publication/manifestation_identifier/PUB_QA0219516ENN>.

[73] Cartwright 167.

[74] Although this point is considering the vitiating factors enabled by smart contracts' anonymity to be precise there is another issue to highlight affected by the anonymity of the parties to a smart contract which is the applicable jurisdiction. Farell et al refer to cross border issues distinguishing between the location for the smart contract and the location of the property to which is linked a smart contract. See Scott Farrell, Heidi Machin and Roslyn Hinchiffle, 'Lost and Found in Smart Contracts Translation - Considerations in Transitioning to Automation in Legal Architecture' (2017) 10-11 <https://www.uncitral.org/pdf/english/congress/Papers_for_Programme/14-FARRELL_and_MACHIN_and_HINCHLIFFE-Smart_Contracts.pdf>.ty

[75] Filatova 229-39.

and the specific asset or token that is the object of the contract. Taken to an extreme, Werbach and Cornell consider that "[t]he parties to a smart contract, at a technical level, are not people. They are cryptographic private keys".[76] Moreover, it is not limited the number of accounts, wallets or keys that any given subject can have,[77] and also "[i]t is also possible for a private key to be under the control of more than one person".[78] So far, prior communications between the parties in the case of long-distance contracts have been decisive for the assessment of the mistake,[79] but in smart contracts it remains to be seen how these prior relationships are materialized and to what extent algorithms are involved in them.

"[C]ontractual capacity is premised on legal personhood",[80] and corporations can act in the same manner a natural person of full age and capacity within the realm of their statute. Contracts can be void, voidable or unenforceable depending on contractual incapacity.[81] The pseudo-anonymity of smart contracts can undoubtedly have consequences arising from the lack of knowledge about the legal capacity of the parties. This lack of disclosure operates in the same way as mentioned above, depending on the type of smart contract.[82]

4.2. *Vitiating factors enabled by code*

But not only does anonymity pose a challenge for the identification of vitiating factors, but also the lack of understandability of the code can enable them. "Making a mistake about the terms of the contract is not really a case of 'mistake' at all, but of the absence of agreement in the formation of the contract".[83] One of the main challenges in relation to mistake and smart contracts is that the party who has made a mistake seeks rectification of the contract, of the document itself, but this is not possible in the case of smart

---

[76] Werbach and Cornell 159.

[77] ibid 160. There is an additional threat to consider in relation to the lack of exclusivity in the relationship between any specific subject and its cryptographic signature, and it is precisely the use of multiple wallets with different public keys that is used specifically to circumvent traceability. See Nathan Fulmer, 'Exploring the Legal Issues of Blockchain Applications Note' (2018) 52 [i], 186 <https://heinonline.org/HOL/P?h=hein.journals/aklr52&i=185> accessed 25 March 2021.

[78] A Veerpalu et al, "The hybrid smart contract agreement challenge to European electronic signature

regulation" (2020) 28 International Journal of Law and Information Technology 39, 74.

[79] Cartwright 169.

[80] Mik, *The Resilience of Contract Law in Light of Technological Change* 6.

[81] Andrew, Beatson FBA and Cartwright 237.

[82] See n 75.

[83] Cartwright 164.

contracts given their immutability. Thus, not only is it difficult to identify the presence of the mistake, sometimes until the contract has been executed, but also, if the mistake was initially identified, it is not possible to rectify the error itself, and in this sense it is irrelevant whether it is a common or a unilateral error.

The same situation applies to cases of misrepresentation, where the mistake was induced by the favored party, either negligently or fraudulently. In smart contracts, the contract cannot be avoided retrospectively due to the immutability of smart contracts. On the contrary, Raskin argues that with smart contracts "[s]ome of the most difficult problems of early contract law" such as misunderstanding and mistake could be potentially minimized due to the use of computer code.[84] But it is yet to consider if the "I agree" button or the browse-wrap system will be enough to overcome these issues.[85]

Non-disclosure falls somewhere between mistake and misrepresentation, and the duty to provide pre-contractual consumer information deserves special consideration. On the other hand, situations involving duress, undue influence or the doctrine of unconscionable contracts present the same evidentiary difficulties arising from the test of causation in both traditional and smart contracts, with the only nuance of their execution in an unstoppable way in the case of the latter.

There is a new category of mistake that should be taken into consideration with the use of smart contracts: the mistake derived from the use of the code. This would be the case where the implementation of smart contracts does not match the intention of the parties.[86] O'Shiled argues that it will be needed "to provide a natural language version of the contract to the parties to obtain mutual consent".[87] There is the additional circumstance that in this case the mistake could be caused by a third party, the programmer. Moreover, the error could be caused by a misunderstanding, be due to incompetence or even be intentional.[88] This is not strictly speaking a defect of consent, but this type of mistake is not currently covered as such by contract law. Some argue that one way to overcome this problem may be through direct coding. "[T]he contracting parties (and their lawyers) could reorient the manner in which they express their agreements to facilitate its subsequent translation into code".[89] This is not more than

[84] Raskin 324.

[85] See Mik, *The Resilience of Contract Law in Light of Technological Change* 21-2.

[86] Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' 11.

[87] O'Shields 190.

[88] Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' 11.

[89] ibid 18.

revisiting the idea of the so-called Ricardian contracts[90] or Surden's data oriented contracts,[91] but it is a solution radically opposed to the one proposed by O'Shiled.

4.3. *An initial thought on how to overcome vitiating factors*

As pointed out before, there is no doctrinal analysis around the specificities of smart contracts' vitiating factors, other than a few brief mentions through the literature.[92] Savelyev briefly refers to vitiating factors highlighting the irrelevance of the presence of vitiated consent for smart contracts' performance.[93] He argues that expression of intent contained in a smart contract has to prevail over the actual intent, because undoing ex post the 'single version of trust' contained in the blockchain, would undermine the capacity to build trust of the smart contracts built on blockchain technology.[94] But we must not lose sight of the fact that Savelyev's view is that users of smart contracts may be looking to use alternative regulatory systems rather than conforming to classic contract law.[95] However, this argument fails because it is not up to the users to decide whether or not to subject their acts to the law, and therefore one of the drawbacks of smart contracts is the one related to the verification of the concurrence of defects of consent. As Agnikhotram and Kouroutakis said "the legal system may not accept [the automation of enforcement] as a feasible solution to the legality of smart contracts".[96]

Some of these challenges might be addressed through "pre-identifiable and trusted processing nodes",[97] able to work on the correct identification of the parties involved in the contract. More complex is the solution to the problems related to mistake in any of its versions, or duress. In relation to them, it is ultimately a problem of proof as it is in the analogical world with the only nuance that the execution of the smart contract cannot be stopped and it is necessary to look for remedies, that as Raskin points out "would again either be in damages or in policing the use of such vending machines before the contract

[90] See I Grigg, 'The Ricardian Contract' (2004) 25-31. Ian Grigg, 'On the Intersection of Ricardian and Smart Contracts' (February 2015) <https://iang.org/papers/intersection_ricardian_smart.html> accessed 2021.

[91] Harry Surden, 'Computable Contracts' (2012) 46 629, 629-700 <https://scholar.law.colorado.edu/articles/148> accessed 26 March 2021.

[92] See e.g. Werbach and Cornell 371. Cuccuru 191.; Eenmaa-Dimitrieva and Schmidt-Kessen 16.

[93] Savelyev 19.

[94] ibid.

[95] ibid 11.

[96] Agnikhotram and Kouroutakis 317.

[97] Cuccuru 192.

could be formed".[98] I argue that legal design to overcome these hazards will require further technical and legal analysis.

III. DEHUMANIZING THE CONTRACT FORMATION PHASE IN SMART CONTRACTS: ALGORITHMIC SMART CONTRACTS

In the previous section, the legal fit of the legal requirements of contract formation for smart contracts to be legally enforceable was analyzed, but only from the perspective of mixed-analog smart contracts or in those cases in which the offer has been deployed on the blockchain in an irrevocable and binding way for the offeror. But an analysis of contract formation cannot be closed without considering those situations in which algorithms determine the obligations of the contracting parties. This is the case where so-called algorithmic contracts enter the arena of smart contract formation.[99] Scholz already said in 2017 that "[s]ome contracts are algorithmic because the parties used algorithms as negotiators before contract formation, choosing which terms to offer or accept".[100] Although "In the context of contract law, technical details are rarely (if ever!) relevant",[101] undoubtedly, algorithmic trading has implications for the legality of smart contracts that must be analyzed independently.

"Computers are programmed to trade without human oversight, to respond to market information in real-time and to enter into transactions when certain pre-set conditions are met".[102] In this sense, the fulfillment of the offer and acceptance requirements may have a legal fit in algorithmic smart contracts since the system will be limited a priori to matching the indications with which the algorithm has been programmed. In that sense algorithms are understood as 'mere tools'. The difference lies in the fact that contract law is not designed for those cases in which the contracting party outsources the process of evaluating the possibilities in the pre-contracting phase to an algorithm. This second type of algorithms are classified for Scholz as 'artificial agents'.[103] She points out two potential problems with respect to algorithmic contracts. First, that the results achieved by the algorithm are not those that would foreseeably have been achieved by the subject on

[98] Raskin 325. Raskin refers to vending machines because it is the visualization that Szabo once made to explain the mechanism of operation of smart contracts. See Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets'.

[99] Lauren Henry Scholz, 'Algorithmic Contracts' (2017) 20 vol 20 <https://papers.ssrn.com/abstract=2747701> accessed 30 March 2021.

[100] ibid 128.

[101] Mik, *The Resilience of Contract Law in Light of Technological Change* 3.

[102] ibid 4.

[103] Scholz, 'Algorithmic Contracts' 135.

whose behalf it acts, and second, the possible illegality of the solutions adopted by the algorithm.[104]

Algorithms can also be classified not only due its role in contract formation, acting as mere tools or artificial agents, but also Scholz distinguishes them in relation to the task assigned, namely gap-filling or negotiation, and moving even further, she differentiates between clear box and black box algorithms depending on whether the outcome of the decision taken by the algorithm can be anticipated or not by its principal.[105] Mere tools and gap-filling algorithms have a more straightforward legal fit with contract law. But the situation varies considerably when we are dealing with algorithms that act as negotiators, especially in the case of black box algorithms.

"Machines and computer programs have no intent".[106] Mik also raises this concern saying that "[g]iven the absence of direct human participation in automated transactions, there is no 'meeting of the minds' and no intention".[107] This statement raises the issue of the absence of human intention and how to conduct automated intention in compliance with contract law. Although her initial concerns, Mik concludes that intention is also present on smart contracts because programming the computer is the equivalent of human intention.[108] Computers are mere tools, and from the objective theory of contract approach of contract law stated before, what is important is the manifested intention, or outward aspect of the intention, meaning that is able to reach the other party.[109] For Scholz there is no problem in regards to intention when referring to clear box algorithms because given the fact that their users can anticipate their results, it would be enough "to show intent to be bound to a reasonably firm universe of outcomes",[110] but she also argues that smart contracts based on black box algorithms might not be enforceable for contract law.[111] Mik's argument about equating intention with computer programming also falls down in this scenario.

"Black-box algorithms are computer programs that improve their performance over the time by trying a certain solution, evaluating the outcome, and them modifying that solution

---

[104] ibid 132.

[105] ibid 136.

[106] Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018) 31 889, 906 <https://heinonline.org/HOL/P?h=hein.journals/hjlt31&i=907> accessed 1 June 2021.

[107] Allen and Widdison in Mik, *The Resilience of Contract Law in Light of Technological Change* 4.

[108] ibid 8.

[109] ibid 8-11.

[110] Scholz, 'Algorithmic Contracts' 136.

[111] ibid 149.

accordingly to improve future outcomes".[112] Hence black-box algorithms raise a different set of problems for the formation stage of smart contracts. Unawareness of the outcome is precisely the opposite of conscious intention and therefore "[b]lack box algorithmic contracts present problems for both mutual assent and consideration".[113] We must not confuse the intention to contract, which as stated before, Mik considers to be present in smart contracts,[114] with the intention to be bound by the precise terms of a contract, and which translates into mutual assent on the terms of offer and acceptance. In regards to consideration, "[i]n a black box algorithmic contract, there is an agreement to agree rather than a true bargain".[115] Vitiating factors may also occur in the case of algorithmically formed smart contracts,[116] notwithstanding the fact that in those in which a black-box algorithm has intervened the concurrence of the vitiating factor may be even more difficult to prove.

So far, different approaches have been presented regarding the legal justification for algorithmic decision making for the formation of smart contracts, although none of them are backed up with a strong analysis. Werbach and Cornell claim without much justification that "it is generally easy to view the computers as agents for their human programmers".[117] Mik goes deeper and points out three different approaches a legal justification for automated contracts. First, what she calls 'Separation Theories', by virtue of which computers are attributed contractual capacity; second, 'Agency Theories' in which computers are instruments of the principal; and a third approach that denies "the existence of human intention in automated transactions", but performs the fiction of converting the intention of the algorithm into contractual intent.[118]

A more comprehensive analysis that can be drawn upon is that of Scholz with respect to algorithmic contracts, and although she distinguishes between algorithmic contracts and smart contracts as more code,[119] I am referring to the use of algorithms for smart

---

[112] Lauren Scholz, *Algorithmic Contracts and Consumer Privacy* in Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò, *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2020) 255 <https://doi.org/10.1017/9781108592239>.

[113] Scholz, 'Algorithmic Contracts' 153.

[114] Mik, *The Resilience of Contract Law in Light of Technological Change* 13.

[115] Scholz 156

[116] Scholz refers to them in relation to algorithmic contracts, but her considerations can be transferred to smart contracts where algorithms are involved in the formation phase. ibid 156-7.

[117] Werbach and Cornell 160.

[118] Mik, *The Resilience of Contract Law in Light of Technological Change* 6-8.

[119] Lauren Henry Scholz, *Algorithmic Contracts and Consumer Privacy* (Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò eds, Cambridge University Press 2020) 251 256-7 <http://dx.doi.org/10.1017/9781108592239.014>.

legal contract formation. She shows that, while complying with the requirement of objective intent, formation theory has certain drawbacks. The first issue to take into consideration is that black-box algorithms perform their choice based on an absolute rationalization that leaves aside other factors that affect the human choice beyond the market price. The second drawback she points out is related to uncertainty, since black box algorithms are particularly difficult to monitor in order to minimize possible risks. The third disadvantage is that it may facilitate the avoidance of accountability. and finally, it points to the possible breakdown of the balance between the parties by strengthening the more powerful party that has the use of these tools at its disposal.[120]

The question is how to translate into mutual assent on the terms of offer and acceptance when an algorithm might have change the human intention originally programmed. In order to overcome the drawbacks pointed out by Scholz, she analyzes the possible application of the law of agency by analogy in regards to contract law for algorithmic contracts. The first aspect she highlights is the fact that an algorithm is not a person and therefore lacks "legal interest to make a contract on its own behalf".[121] In order to solve this nuance, she proposes that algorithms, since they cannot be considered human agents, be considered agents without legal personality or quasi-agents, although in this case accountability problems arise with respect to the principal. To this end, she presents three mechanisms to achieve the enforceability of algorithmic contracts by meeting the requirements for contract formation: real time updates, insurance mechanisms, and the introduction of “a human approval node for each transaction”.[122]

Although this approach could solve the theoretical problems regarding contract formation identified with respect to contracts involving black-box algorithms, in my opinion there are certain drawbacks that should be highlighted. Real-time updating or human approval nodes could pose a delay for process automation and rapid decision making that the use of algorithms is intended to overcome. In addition, problems could arise from the delay in ratification of the decision made by the quasi-agent by the approval node, or the impossibility to stop the execution if it has already started if real-time update is applied as a solution. Finally, an insurance mechanism implies neither agreement nor ratification, which are the requirements of agency law to create agency relationships.

As such, although Scholz's approach to the legal validity of the formation of algorithmic contracts can serve as a starting point for the analysis of smart contracts in

[120] Scholz, ‘Algorithmic Contracts’ 158-64.

[121] ibid 164.

[122] ibid 164-7.

which algorithms are involved in their formation, this analysis is considered insufficient and it is necessary to deepen this matter in order to legitimize the formation phase of such contracts for their legal validity and enforceability.[123]

IV. CONTRACTUAL FREEDOM AND CONTRACT FORMALITIES: LANGUAGE AND SIGNATURE

The general rule is that contract law is form free, and its physical representation is not the agreement itself.[124] It is important to distinguish between the substance of the contract, which is the set of rights and obligations agreed by the parties, and its form of expression. In relation to the later, the formality of the written form for certain types of contracts serves a dual purpose, on the one hand for evidentiary reasons as it allows to know the existence of the agreement, its terms and the intention of the parties, and on the other hand, it has a preventive function as it forces the parties to deliberately consider whether they want to be bound by the contract.[125] At this point the premise that "the mere fact that the contract is concluded by electronic means does not mean that it is not a contract",[126] seems to be accurate.

But also the term smart contract relates interchangeably to both, the technology itself, as well as to the applications build on that technology. The former has an operational meaning which is "the computer code stored, verified and executed in a blockchain",[127] it is purely the protocol, also known as "smart contract code".[128] The later "focuses on how legal contracts can be expressed and implemented in software",[129] or how to embed legal contracts on blockchain technology. They are known as "smart legal contracts".[130] Similarly, "[t]he term contract refers both to the agreement and to its embodiment, the document (if any) evincing the existence of such rights and obligations".[131] Hence, if all the requirements outlined in the above sections are met, there is an agreement, which is

[123] It should be noted that the application of Scholz's proposed solution for algorithmic contracts to smart contracts whose formation phase involves black-box algorithms is not part of his analysis and, therefore, its suitability for his algorithmic contracts is not evaluated in this research. Scholz's approach to smart contracts is to consider them solely as code for executing agreements. See Scholz, *Algorithmic Contracts and Consumer Privacy* 254-7.

[124] Mik, *The Resilience of Contract Law in Light of Technological Change* 13.

[125] Andrew, Beatson FBA and Cartwright 80.

[126] Savelyev 11.

[127] Durovic and Janssen 5.

[128] J Stark in Clack, Bakshi and Braine 2.

[129] ibid 2.

[130] Many authors have referred to them as such. See v.g. Durovic and Janssen 5.

[131] Mik, *The Resilience of Contract Law in Light of Technological Change* 13.

a source of rights and obligations and can be embodied both as a traditional contract and as a smart legal contract.

However, if the absence of specific required form is the general rule, a detailed analysis of the smart contract must also consider those exceptions in which an instrument in the form of a deed is mandatory for the transaction to be valid, such as the case of a gratuitous promise, and those in which written form is required, such as contracts of guarantee or contracts for the sale of other disposition of land.[132] There is no much assessment of smart contracts' form requirement in legal literature. Some scholars briefly refer to contractual freedom,[133] and some comments are made in relation to the evidentiary nature of the written document as opposed to the difficulty for judges to interpret the code contained in the smart contract.[134] There is no problem from the point of view of the written form requirement in those smart contracts, which we have referred to as mixed-analog-smart, because compliance with the written form requirement is covered in its analog part and the 'smart' part is provided only for the execution of certain parts of the agreement.[135] Yet, certain adaptations of legislative provisions will be necessary to accommodate smart contracts within the framework of deeds.

Although some parallelism could be drawn between digital contracts or e-commerce and smart contracts in order to justify the legal validity of the later, there is a significant difference between e-commerce agreements and smart contracts which weakens this argument: despite their digital form, e-commerce agreements are "written in natural language".[136] Hence this parallelism can only be argued with respect to so-called mixed-analog smart contracts, but no in regards to pure smart contracts.

Mik said that "code and natural language are equally valid forms of expression",[137] and the implications of the use of different contracting languages has been broadly object of analysis and regulation on regards of international commercial contracts.[138] The majority opinion of the authors is that in case of discrepancy between the code and the original traditional contract of which the smart contract is a translation, the one written in natural language should prevail, but this presents certain difficulties. The first and most obvious

---

[132] Andrew, Beatson FBA and Cartwright 80-94.

[133] See e.g. Durovic and Janssen 12. Agnikhotram and Kouroutakis 311.

[134] Eenmaa-Dimitrieva and Schmidt-Kessen 15.; Agnikhotram and Kouroutakis 315.

[135] Mateja Durovic and Franciszek Lech, 'The Enforceability of Smart Contracts' (2019) 1 73, 506.

[136] Agnikhotram and Kouroutakis 315. Code vs Natural language is the difference highlighted here because this point refers specifically to the form of the contract, but another significant difference stated in chapter 1.4. is that E-commerce performance is not digitally executed either. It requires human intervention. See Caria 742

[137] Mik, *The Resilience of Contract Law in Light of Technological Change* 13.

[138] See e.g. Filatova 230. Farrell, Machin and Hinchiffle 4.

difficulty is that it does not apply to contracts written directly in code, in which the discrepancy between what the parties wanted and what is reflected in the code must be resolved by means of mistake or misunderstanding as a vitiating factor. The second concern is whether using code can be considered equivalent to writing in human language. This is an issue that in principle would only affect the evidentiary nature of the matter, since there is no specific requirement for communications between the parties to be in natural language.[139]

Compliance with the form requirement of the contract may also be affected by issues relating to the signing of the contract. As pointed out before, "[d]eploying a smart contract to a distributed ledger and signing the smart contract with a private key should constitute a valid offer and acceptance".[140] To date, electronic signatures are admissible as evidence, but neither the EU eIDAS on electronic identification and trust services for electronic transactions in the internal market, nor the UK's Electronic Communications Act give them direct legal validity. In this regards, although applying these principles and policies to cryptographic keys can be considered equivalent to electronic signatures, and in that sense have legal recognition, "and so cryptographic signature should be sufficient",[141] this statement has certain nuances.

The first nuance that we have to take into consideration is that smart contracts built on blockchain technology are anonymous and that we should not confuse it with privacy. Blockchain is "asymmetrically encrypted"[142] what means that it has a two-steps verification system which in practice involves that each user holds both, a public and a private key, mathematically related "by virtue of which the private key can decrypt data that has been encrypted through the public key".[143] The public key is the one that, shared with another user, enables the transaction. Anonymity undoubtedly raises liability issues that do not apply to e-commerce.[144]

The second nuance to consider is that there is no absolute identity between an individual and his key. Any given individual may hold countless keys, "enter transactions using a new digital identity each time",[145] and therefore "the person and the key are not

[139] Durovic and Lech 501.

[140] 'Smart Contracts: Is The Law Ready?' 14.

[141] Durovic and Lech 497.

[142] Berberich and Steiner 422.

[143] Finck 26.

[144] The a priori pseudo-anonymity implicit in smart contracts may result in the impossibility of identifying who to sue in the event of malfunction or unpredictable outcome of the smart contract. See Fulmer 185.

[145] Filatova 220.

the same".[146] This also does not apply to e-commerce. But, to partially counteract these drawbacks derived from anonymity, two requirements are considered relevant in cyberspace, and therefore could be equally applicable to smart contracts, namely authentication and authorization. The first refers to proof that the subject is who he claims to be, and the second, that the subject has the necessary permission to do what is required.[147] In both cases the cryptographic key would serve this function because it links the particular token to the user of the key.

Moving forward "[p]roblems arise when online interactions move from screens and keyboards to a multitude of voice, touch and gestural interfaces".[148] Going beyond the current state of the art, the use of cryptographic keys could be facilitated by sensory systems, and just as the click-to-sign requirement has done for e-commerce, cryptographic key interfaces might evolve in a similar direction as a result of ubiquitous computing and therefore new formality concerns might arise.

V. CONCLUSIONS

Although there is widespread agreement that the formation phase of smart contracts can conform to the principles of contract law,[149] as this paper has shown, not all requirements fit automatically and the assessment of the legality of smart contracts requires a detailed analysis of each of them. The application of the objectivity theory simplifies the requirement of offer and acceptance, and especially when it has occurred offline. Acceptance could also occur online after the offer has been deployed on the blockchain and the signing of a smart contract through a cryptographic key proves that the parties have reached an agreement. It is yet to be determined whether some inconveniences could arise due to the delay in generating new blocks, or in ratifying the agreements reached by the algorithms.

Intention and consideration have also been the subject of examination. In relation to the first of these requirements, different scholars analyze the concept from different angles: from the intention to be legally bound, the intention to be subject to the exact terms of the contract and even the intention to use an alternative system. Regarding the second requirement, this is a more contentious issue. The range of possibilities extends from those who consider that because there is an exchange between the parties there is consideration, to those who consider that because of its automation, there is no

[146] Werbach and Cornell 160.

[147] Eenmaa-Dimitrieva and Schmidt-Kessen 32.

[148] Mik, *The Resilience of Contract Law in Light of Technological Change* 22.

[149] Durovic and Janssen 10. Raskin 322.

commitment to do anything. Vitiating factors require special consideration in smart contracts as they can be facilitated by both the anonymity of the contract and the use of code. Anonymity also brings problems in regards to jurisdiction and the decentralization nature of the blockchain ledger makes difficult to determine where a smart contract has been formed in order to determine which law is applicable in enforcing the agreement.[150]

It is not that clear that smart contracts might satisfy contract law requirements for contract formation when algorithms play the leading role in the formation phase of smart contracts. “Current contract law presumes algorithms are mere tools, executing the will of their owners directly, with no ability to learn or decide. This is demonstrably not true in many algorithms that are used in contracts today”.[151] As a result, the study on the law of agency with respect to Scholz's algorithmic contracts has been considered as a good starting point for the analysis, but this has proved to be insufficient, being necessary further analysis.

Finally, the form of contracts has also been considered in this paper since, directly related to the contract formation phase, the principle of freedom of contract presents certain peculiarities in its interpretation with respect to smart contracts, analyzing the possible consideration of code as a valid language as well as the concurrence of the requirement of signature through cryptographic keys.

[150] Fulmer 185.

[151] Scholz, ‘Algorithmic Contracts’ 132.

THE SOCIAL NETWORK PROFILE SHUTDOWN IN THE DIGITAL IDENTITY PERSPECTIVE

Por

EDOARDO VINCHESI
PhD Candidate at the Università Ca'Foscari Venezia

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

ABSTRACT: The paper summarized in this abstract takes its cue from some recent court decisions, in particular the judgement of the Court of Bologna on March 10th , 2021, under which the event of the digital profile cancellation without justification has been recognized as cause to the right to a compensation for the non-patrimonial damage (according to the article 2059 of the Italian Civil Code), even though the digital profile cancellation is expressed only in a generic manner in the contractual terms (or conditions of use) of the social network, with an evident risk of abuse.

KEYWORDS: Personal Identity, Digital Identity, Social Network, Social Profile Shutdown, Legibility.

SUMMARY: I. INTRODUCTION. II. THE CASE. III. THE DIGITAL IDENTITY IN THE PRISM OF PERSONAL IDENTITY. IV. THE NETWORK ACCESS CONTRACT. V. THE RIGHT TO EXPLANATION IN RELATION TO THE ALGORITHM, THE THEORY OF LEGIBILITY IN THE SPECIFIC CASE. VI. FURTHER CONSIDERATIONS. 1. Unfair commercial practices within the network. 2. Protecting the digital profile of companies

EL CIERRE DEL PERFIL DE LA RED SOCIAL EN LA PERSPECTIVA DE LA IDENTIDAD DIGITAL

RESUMEN: El presente trabajo se inspira en algunas decisiones judiciales recientes, en particular la Sentencia de la Corte de Bolonia (10 de marzo 2021) bajo la cual se ha reconocido la cancelación de perfiles digital sin justificación como causa para el reconocimiento del derecho a una indemnización por daños no patrimoniales (de conformidad con el artículo 2059 del Código Civil italiano), puesto que la cancelación del perfil digital se expresa sólo de manera genérica en los términos contractuales (o condiciones de uso) de la red social, con un riesgo evidente de abuso.

PALABRAS CLAVE: Identidad Personal, Identidad Digital, Redes Sociales, Cierre de Perfiles Virtuales, Comprensibilidad.

I. INTRODUCTION

The subject starts from the appeal ex art. 702 ter cpc (the Italian code of civil procedure), in the case DGV vs Facebook Ireland Limited, in front of the Bologna Civil Court, dated 10th March 2021. The aim of the present paper is to analyse the possible implications of the non-patrimonial damage in case of lesion to the digital identity, in particular in relation with the social networks and the digital *platforms*. In order to analyse the juridical issues related to this specific case, a brief summary of the facts will follow.

II. THE CASE

The applicant part explained, with appeal ex art 702 bis c.p.c. (as explained in the Italian civil procedure code, this particular act allows the judge to decide very quickly, even with precautionary measures), that he subscribed to Facebook 10 years before through a page that was connected to his name and surname, that were used as an account for other two social pages, called «*Collezionismo militare e legge*» and «*Libri e riviste storia militare*», both cancelled in January 2020.

In particular, he underlined the fact that the counterpart did not give any explanation while the profile was cancelled. Furthermore, the part - currently exercising as a lawyer - explained that he was acting as barrister for another case, that involved the same Irish company (again, as the counterpart) also regarding the closure of the digital profile of another user. For this reason, the part had submitted a *diffida* (an act of warning often necessary in order to start civil trials in the Italian order) only 20 days before the closure of his digital profiles. Therefore, he claimed that the conduct of the *social network* was an act of retaliation.

Having said that, the part asked, as a consequence, that the same Company reopened the above-mentioned profiles and pages, establishing a penalty for each day of delay, and a refund of damages.

In deciding about the situation, the implicit aspects of the question are briefly exposed, these aspects being the patrimoniality of the relationship (for the judge, undoubtably a relevant aspect) and the abstract possibility of the subsumption of the act made by the social network in the art. 1218 c.c. (the basis of the contractual damage, as explained in the Italian civil code), seen that the behavior of the social network should be considered a breach in the obligation.

Furthermore, it has been highlighted that according to the contract between the parts (accepted by the user once he subscribed), the possibility of closing the profile is mentioned, but only as a consequence of a continued violation of community standards, and (even more important) after warning the user.

In addition, the destruction of any means of proof relating to the present case, by express admission of the defendant, and also the impossibility of reconstructing the reasons which led to the cancellation of the profile, appeared particularly serious elements in favor of the applicant.

The defendant's objection that the counterpart was responsible for having waited too long (seven months) to initiate the procedure was found to be irrelevant, since it had to be considered - on the contrary - as a not excessive period of time. In any case, in addition to having recalled the simplicity of the preservation of the evidence, especially when of a digital nature like in the present case, it was also recalled that the burden of proof of the non imputability, on the basis of the art. 1218 c.c., it could only fall on the social network.

Moreover, the issue of possible retaliation was not even challenged by Facebook.

The decision of the Bologna Court also appears to be worthy of appreciation where, having regard to the need for a source justifying the claim for compensation for non-material damage, points out that such an offence appears to be worthy of compensatory satisfaction where a right of the person protected by the Constitution has been seriously infringed and makes it clear that "*place that the reference on the art. 2059 c.c. to the cases in which the law allows the compensation of the non-patrimonial damage well can be reported, after the Italian Constitution, also to the decisions of the fundamental law, even when it results from a breach of contract (Italian Supreme Court n. 26972 of 2008), there can be no doubt that the right to carry out one's own relationship life and the right to freely express one's own thought constitutes fundamental rights of the person, constitutionally guarantee*"[1]. And this exercise can be manifested through social media, not interfering with the constitutional relevance of these rights, but rather, having to appreciate the importance, given their use by about 2,7 billion users, and their importance since individuals even through social media can well "*use them for the purposes of projecting their identity, weaving personal relationships, expression and communication of their thought*"[2] and the damage generated by the relationship life could not be - moreover - amended by the opening of a new profile.

But a first point of relevance, starting from the above-mentioned considerations, already emerges. In fact, the pronunciation does not directly mention the articles of the Italian Constitution that have to be taken as a reference to legitimize the recognition of the

[1] In the Italian version: *posto che il rinvio di cui all'art. 2059 c.c. ai casi in cui la legge consente il risarcimento del danno non patrimoniale ben può essere riferito, dopo l'entrata in vigore della Costituzione, anche alle previsioni della legge fondamentale, anche quando derivi da un inadempimento contrattuale (Corte di cassazione Sez. U., Sentenza n. 26972 del 2008), non può dubitarsi che il diritto di svolgere la propria vita di relazione e il diritto di manifestare liberamente il proprio pensiero configurino diritti fondamentali della persona costituzionalmente garantiti.*

[2] In the Italian version: *utilizzarli per i fini di proiezione della propria identità, di intessitura di rapporti personali, di espressione e comunicazione del proprio pensiero.*

non-material damage in favour of the applicant, mentioning - rather - the ontological aspects, and identifying it in two aspects: freedom of thought and digital identity.

For the first one, the Article 21 of the Italian Costitution is easily identifiable for the interpreter, but it does not seem to be so for the latter. In fact, while recognizing a basis in art. 22 of the Constitution, personal identity (of which digital identity constitutes development and declination) goes far beyond the mere right to name, expressly mentioned in the norm.

From here it is worth starting to develop additional considerations.

III. THE DIGITAL IDENTITY IN THE PRISM OF PERSONAL IDENTITY

The matter analysed by the Bologna Court does not only highlight issues such as non-patrimonial damage, the legal relationship between user and social networks, fairness - or good executive faith - in the relationships between the parties and the relationship between user and algorithms (or automated procedures in general), but also that of the digital identity of the individual, also and above all with respect to the safeguards that the Italian legal system allow in this regard.

In fact, digital identity[3] distinguishes from personal identity as it develops inside the web, while maintaining its underlying characteristics and the latter deserves distinction from the right to name[4].

---

[3] Considerations on this topic have been expressed by: G. ALPA, *L'identita` digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, Padova, 2017, p. 723 ss.; G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003, *passim*; P. MICHEA DE BERTI, J. FRANCHINI FORLANI, *Osservatorio comunitario: La corte di giustizia riconosce alle persone interessate il "diritto all'oblio" dei propri dati personali*, in *I contratti*, VII, Assago, 2014, p. 716 ss. ; A. VERDESCA E I. STELLATO, *Diritto all'oblio e pubblicità commerciale: un bilanciamento invertito*, in *Il Corriere Giuridico* n. VIII - IX, Assago, 2018, p. 1129 ss.; A. SIROTTI GAUDENZI, *Diritto all'oblio e diritto all'informazione: un difficile equilibrio,* in *Il Corriere Giuridico* n. VIII - IX, 2018, p. 1107 ss.; M. M. MOLLICONE, *il registro delle imprese conserva i dati di amministratori/liquidatori salvo eccezione,* in *Giurisprudenza Italiana*, VI, 2018.; M. DOGLIOTTI, *Persone fisiche, capacità, status, diritti* in *Trattato di Diritto Privato*, M. BESSONE (*a cura di*), Torino, 2014, *passim*; V. ZENO ZENCOVICH*, voce «Identità personale*", in *Digesto IV ed., Disc. priv., sez. civ.*, IX, 1993, p. 300 ss.; P. MICHEA DE BERTI, J. FRANCHINI FORLANI, *Osservatorio comunitario: La corte di giustizia riconosce alle persone interessate il "diritto all'oblio" dei propri dati personali*, in *I contratti*, VII, Assago, 2014, p. 716 ss. ; A. VERDESCA E I. STELLATO, *Diritto all'oblio e pubblicità commerciale: un bilanciamento invertito*, in *Il Corriere Giuridico* n. VIII - IX, Assago, 2018, p. 1129 ss.; A. SIROTTI GAUDENZI, *Diritto all'oblio e diritto all'informazione: un difficile equilibrio,* in *Il Corriere Giuridico* n. VIII - IX, 2018, p. 1107 ss.; M. M. MOLLICONE, *il registro delle imprese conserva i dati di amministratori/liquidatori salvo eccezione,* in *Giurisprudenza Italiana*, VI, 2018; p. 1526 ss. R. TOMMASINI, *L'identità dei soggetti tra apparenza e realtà: aspetti di una ulteriore ipotesi di tutela della persona*, in *Il diritto all'identità personale*, ALPA-BESSONE-BONESCHI (*a cura di*),1981, p. 83 ss.; M. DOGLIOTTI, *Il diritto alla identità personale nel quadro dei diritti della personalità*, in *Il diritto all'identità personale*, a cura di Alpa-Bessone-Boneschi,1981, p. 68 ss.; V. ZENO ZENCOVICH*, voce "Identità personale"*, nel *Digesto IV ed., Disc. priv., sez. civ.*, IX, 1993, p. 300 ss.

[4] R. TOMMASINI, *L'interesse alla riservatezza ed i valori della persona di fronte alla libertà di manifestare il pensiero*, in *L'informazione e i diritti della persona*, ALPA-BESSONE-BONESCHI-CAIAZZA

Starting the analysis from this last aspect, it is necessary to briefly recall the salient features of the right to name, in particular the staticity that distinguishes it, summarizing itself in the right for the individual to not be seen outside (or in the social context in general) tarnished or misrepresented in his identifying traits[5].

If the right to the name embraced therefore a static vision, classification of the individual's identity constitutes its natural evolution, as well as - under the social context point of view - the individual himself has found new spaces to define and assert himself, evolving in its turn and thus being able to autonomously define its identity, even imposing itself towards the community with the traits that he attributed to himself[6]. Before declining these concepts in the digital reality (in which they manifested with disruptive force) is appropriate to consider, for example, the gender identity, today linked to a real feeling of the individual, avoiding the pre-ordering static that society has known in the past[7].

Well, starting from the view of the dynamic nature of the right to identity, as well as the strength of definition of the traits attributed to the individual, and which so greatly separate this concept from his chrysalis, the right to name, from which it was born by gemmation[8], even more disruptive was the appearance on the legal scene of the right to digital identity.

If in that circumstance, as in the case of the right to personal identity *tout court*, is confirmed the self-declination of individual traits, the speed of the evolution typical of the world wide web and the digital reality has accentuated even more this aspect.

As an example, consider the mutability of the activity of browsing on the web, being an user able to pass in an instant from digital consumer in an e-commerce site and then sell, himself, something in the same digital platform; still, in an instant one can switch from the social profile - as "mere" user - to manage a page on the same site (or even in a different

---

(*a cura di*), 1983, p. 40 ss.; G. PONZANELLI, *Alcune novità in materia di diritto al nome*, in *Giur. It*., 1981, I, p. 380 ss.; A. FUSARO, *Nome e identità personale degli enti collettivi. Dal diritto all'identità uti singuli al diritto all'identità uti diversi,* in *La nuova giurisprudenza civile commentata,* XVIII, 1⁄2, Padova, 2002, p. 51 ss.; M. A. LIVI, *Il diritto al nome nel prisma dell'identità personale*, Milano, 2012, p. 22 ss.; S. PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 1962, p. 50 ss.

[5] Cassazione 22.06.1985, n. 3769, V. ZENO ZENCOVICH, in *La nuova giurisprudenza civile commentata*, 1985, I, p. 647

[6] A. FUSARO, 2002., p. 51 ss.

[7] Even more important appears this consideration to be regarding the topic of the change of sexuality without surgical operation, as established by the Messina Court, 11.11.2014, in fact (in original): "*Il diritto all'identità sessuale va pienamente riconosciuto non solo a coloro che, sentendo in modo profondo di appartenere all'altro genere, abbiano modificato i loro caratteri sessuali primari, ma anche a coloro che senza modificare i caratteri sessuali primari abbiano costruito una diversa identità di genere e si siano limitati ad adeguare in modo significativo l'aspetto corporeo.*" In NGCC 2015, I, p. 543 ss. In general, about the topic consider also: A. VESTO. *Il genere: identità,, filiazione, genitorialità*, S. CACACE, NGCC 7-8/2018, p. 1168 ss.

[8] Or "concentrical holes" as expressed by G. PONZANELLI, 1981, p. 380 ss.

one), arriving in the latter case to have to answer also about the data or the activity of other registered users.

In the latter sense, the jurisprudence has had the opportunity to clarify[9] how the blogger, due to his qualification as a "provider of web space" is to be considered as an hosting provider, carrying out an activity of "storage of other people's content"[10], having to reject the idea of a general obligation of vigilance[11] at the expense of the platform. Nevertheless, in some cases the blogger will respond to the service user[12]. Note, however, that this opinion is not without criticism according to the most cautious Doctrine[13].

The theme of identity, expressly mentioned in the pronunciation from which the present work has taken its cue, ultimately embraces the individual in its entirety, becoming concrete in the declination that he wants to give of himself, particularly in the digital and social context, also because the pervasive force of such platforms in daily life cannot be ignored.

If the pronunciation, as previously mentioned, omits to highlight the individual constitutional articles that protect the identity of the person, this (not easy) assignment is for the interpreter to do, according to the fact that from time to time he will be called to identify the reference standard.

In the present case, freedom of expression of thought has been highlighted, a theme that opens the doors to the issue of the contractual relationship between the individual and the social networks as a way for the expression of digital identity.

---

[9] In particular with the following pronunciations: Cassazione, n. 12546, 2019, in *Ced Cassazione*; Cassazione, *sezione* V penale, n. 54946, 2017, in *Ced Cassazione*; Cassazione, *sezione* III penale, n. 5107, 2014, in *foro it.*

[10] D. MINOTTI, *Valutato come attivo un comportamento solo connivente*, Sezione V penale, Sentenza 8 novembre 2018 - 20 marzo 2019 n. 12546, in *La Guida al Diritto*, XX, 2019, p. 91 ss.

[11] Art. 15 Directive 2000/31 CE transposed with the D. Lgs. 70/2003 art. 17.

[12] The blogger won't be held responsible if he doesn't know about the conduct and if - as soon as he is informed about it - he intervenes. In the Italian version of the law: "*Non risponderà pertanto*, il *blogger* (o l'*hosting provider*) purché, come chiarito dall'art. 16 del decreto e 14 della direttiva di cui alla nota precedente "*a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso*".

[13] D. MINOTTI, 2019, p. 91 ss., in particular it appears clear that a responsibility based on this causes has the only purpose to sanction the most vulnerable individual, since the impossibility to identify the real author of the comment. In the original version: "si *impone a un operatore (il blogger) un improbabile ruolo di arbitro che deve procedere a un bilanciamento di interessi tra reputazione (e riservatezza) della pretesa persona offesa e libera espressione del pensiero del commentatore*".

IV. THE NETWORK ACCESS CONTRACT

The contract between user and social networks has created wide debates within the Doctrine, which has proposed several reconstructions.

For some scholars[14], the contract in question should be distinguished from the IP identification system provided. With the risk - however - of attributing to a merely executive role (such as, precisely, that of providing the IP address) a nature different from that which in practice belongs to him[15].

According to a different view, such a case would be included among the access contracts to the Internet network[16], thus not distinguishing itself from the contracts that perform services inherent - for example - to the e-mail service or those that provide the connection service tout court.

Moreover, for a different thesis, it should be applied the law of the procurement contract; for a different view would be applicable, instead, the discipline of the administration contract[17].

The role of the platform appears in any case to be different from that of the service provider, as is known as purely passive. This, rather than dealing with the provision of the user's connection service, takes care - in fact - of his data and, in particular, on how users themselves come into contact with each other, thus allowing the exchange of information between them[18].

---

[14] G. DE NOVA, *Relazione al convegno su "Internet, Profili Giuridici*", Pavia, 4-5 Ottobre 1996, in *Aida*, 1996, p. 39

[15] N. VISALLI, *Contratto di accesso ad internet e tutela della privacy*, in *Giust. Civ.*, II, 2002.

[16] M. GRANIERI, *Le clausole ricorrenti nei contratti dei social network dal punto di vista della disciplina consumeristica dell'Unione Europea*, in *Aida, Annali Italiani del Diritto D'autore, della Cultura e dello Spettacolo*, 2011, p. 125 ss. About the consequences of the consideration of the user of the social network as a consumer consider also G. G. CODIGLIONE, *pere dell'ingegno e modelli di tutela*, Torino, 2017, p. 359 ss.; F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attivita` economica*, Milano, 2018; V.RICCIUTO, *Nuove prospettive del diritto privato dell'economia*, in E. PICOZZA E V.RICCIUTO, *Diritto dell'economia*, II ed., Torino, 2017, p. 345 ss; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. e Impresa*, III, 2018, p. 1088 ss.

[17] For the firs thesis N. VISALLI, 2002*.,* p. 125 L. ALBERTINI, *Il contratto di accesso ad internet*, in *Giust. Civ*., II, 1997, p. 102 ss.; for the second one R. BOCCHINI, *Il contratto di accesso ad internet*, in *Dir. Inf.*, 2002, p. 485. In general, the central aspect of the consideration is probably - as the two authors have underlined - the duration of the contract.

[18] The topic appears to be, shortly, the importance of the algorithm, and how user's data are used by it. According to such a disruptive conduct it appears hard to consider the platform as a mere *Internet Service Providers*. (G. SARTOR, *Social networks e responsabilità del provider*, in *Ann. It. Dir. Aut.*, 2001, p. 43). Differently, about the eco-chambers topic is possible to mentioned A. MASERA, G. SFORZA, *internet, i nostri diritti, a cura di Stefano Rodotà*, Bari, 2016; D.C. NUNZIATO, *Virtual freedom: net neutrality and free speech in the internet age*,, California, 2009; M. VILLONE, *La costituzione e il "diritto alla tecnologia"* in G. DE MINICO (a cura di), *Dalla tecnologia ai diritti*, Napoli, 2010, p. 267; M. BARBERIS, *come internet sta uccidendo la democrazia, populismo digitale*, Milano, 2020, *passim.*

Moreover, it seems possible to doubt about the mere and simple juxtaposition between the two activities, considering, however, the tripartition of responsibility provided by Legislative Decree no. 70/2003 in the matter, limited to mere conduit, caching and hosting activities[19]. In relation to these, the ISP is exempted from a general monitoring obligation[20].

In short, for part of the Doctrine, the difference between the two activities exercised by the social platform and the ISP seems to be the main element in order to consider a difference between the contract of access to the network and the contract by which the user is allowed to register and use the social platform itself[21].

Another issue, in addition to identify the type of contract on which the relationship between user and social is based, is that of gratuitousness or onerousness of the contract in question, for the particular tightening of the execution to which the activity of the platform will have to conform if the second thesis prevailed.

For some authors[22], differently, the very nature of the service offered (as mentioned, intrinsically different from that of mere access to the Internet) is an element to affirm the gratuitousness of the contract in question. The platform, in fact, would be limited to provide a virtual space dotted with advertisements, and only from the latter would receive a fee of an economic nature.

Within this debate there is an appreciably detailed thesis of that part of the Doctrine which sees in the reconstruction of this report a mere relation of courtesy, considering "*the absence of a direct financial sacrifice of the user for the use of the service*"[23]. This seems, however, disagreeable since, even if one does not want to recognize the nature

[19] M. GAMBINI, *La responsabilità dell'internet service provider*, Napoli, 2006; R. D'ARRIGO, *Recenti sviluppi in termini di responsabilità degli internet services providers*, Milano, 2012; M. IASELLI, *I contorni della responsabilità dell'hosting provider attivo*, in *Il Diritto Industriale*, IV, 2019, p. 399; G. CASSANO, *La Cassazione civile si pronuncia sulla responsabilità dell'internet service provider,* in *Il Diritto Industriale*, IV, 2019, p. 364; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; C. PERLINGIERI, *La responsabilità civile dell'internet provider*, in A. DI AMATO (a cura di), *Appunti di diritto dei mezzi di comunicazione*, Napoli, 2006, p. 247.

[20] Even if a responsibility is possible for specific guarantee obligations; in particular according to the Italian law: "*specifici obblighi in relazione alla posizione di soggetti dotati di particolari conoscenza e competenze tecnico professionali che ne caratterizzano l'attività e nelle quali confidano gli operatori della rete*" (C. PERLINGIERI*, Profili civilistici dei social networks*, Napoli, p. 42 ss.), even about the c.d. abusive linking or "*linking abusivo"* (B. Tassone, *Responsabilità del provider per linking abusivo e criteri di liquidazione del danno*", in *Il Diritto Industriale*, IV, 2019, p. 377).

[21] C. PERLINGIERI*,* 2014.

[22] F. ASTONE, *Il rapporto tra gestore e singolo utente: questioni* generali, in *Ann. It. Dir. Aut.*, 2011, p. 107; P. SAMMARCO, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0*, in *Il diritto dell'informazione e dell'informatica*, IV-V, 2010, p. 631 ss.; W. VIRGA, *Inadempimento di contratto e sanzioni private nei social network*, in *Ann. It. Dir. Aut.*, 2012, p. 219 ss.

[23] P. SAMMARCO, 2010, p. 631 ss.

of synallagmaticity to the relationship between social platform and user, it seems nevertheless undoubted that platforms gain profits from the presence of users, even if indirectly, thanks to advertising.

Therefore, the thesis of the mere relationship of courtesy is to be rejected, since the presence of users seems an undoubted necessity, because advertising notices - from which social networks gain profits - are clearly intended for users themselves.

In any case, the European legislator has expressly stated its position on this debate, with the Directive 770/2019 in fact he has stepped in this discussion. Issued together with Directive 771/2019 the solution represents, together with this one, an element of absolute appreciability[24].

Although no express solution is proposed[25], the problem of the qualification of the relationship between personal data and digital service is addressed; in particular, in the art. 3. Leaving aside the first paragraph (where there seems to be no doubt in defining the relationship as a contract), the second paragraph is of greater interest. However, with regard to that provision, at first reading it would appear that there is a lack of remuneration, about which the Legislator promptly remedies.

The latter establishes, in fact (after dealing with paragraph 1 of the digital supplies for consideration) an extension of consumer protection also to digital supplies "free structure"; is excluded, vice versa, any form of protection in the case of supplies entirely free of charge[26].

In this way, the protection of consumers who access a service by providing, as a counterpart, their data is expressly extended. In this sense, the principle of *primautè* of the European law, which as we know is also reflected in the choice of an interpretation of the rule in accordance with it, seems to make preferable the reconstruction that recognizes free nature to the relationship between user and social, but, nevertheless, expressly requiring the user to get the protection of the consumer discipline.

Recognizing the duty of protection of the user as it would be with the consumer, the obligation of fairness between the parties is highlighted in the subject of the forced clo-

---

[24] C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. Civ.,* III, 2019. In particular, the second one appears to be of huge importance, being an important legal source about digital services.

[25] C. CAMARDI, 2019.

[26] As the directive establishes it "*shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose*" (art. 3 c.2).

sure of the digital profile with even greater force, and in particular it becomes necessary to address the issue of the obligation of information in relation with the algorithm, also on the basis of the theory of knowability (or legibility) in cases like this.

V. THE RIGHT TO EXPLANATION IN RELATION TO THE ALGORITHM, THE THEORY OF LEGIBILITY IN THE SPECIFIC CASE

Recognizing the applicability of the consumer protection to the agreement between user and social is appropriate - on the basis of this corollary - to focus on the agreement signed between the parties.

The consumer status will allow to apply not only the obligation of correctness (or *bona fide in executivis*) between the parts, specifically ruled by the Italian civil code (art. 1375 cc, art. 1175 cc) and the obligation of information that arises from that as development of the principle of good faith[27], but also the Italian consumer code, and in particular the article 2 c.2 lett. c), the article 5 c.3 and the article 35, establishing - according to the different contractual strength of the parties - a greater obligation of clarity and transparency on the strongest part.

According to the most careful Doctrine, moreover, in relation with the algorithm the user-consumer should be protected, according to the need for clarity and good faith, by a real right to the knowability of the configuration - at least in a practical sense - of the algorithm (or, more precisely, the behavior of the algorithm).

For the c.d. theory of legibility in fact it would be necessary (for the strongest part) to ascertain the ability of the subject to independently understand data and analytical algorithms through a concrete explanation of methods and data used[28].

In short, the legibility of the decision would be based on the "comprehensibility of the algorithm" and the "transparency with respect to its use"[29]. Recently, in fact, various

[27] M. BARCELLONA, *L'abuso del diritto: dalla funzione sociale alla regolazione teleologicamente orientata del traffico giuridico*, in *Riv. Dir. Civ.*, II, 2014, p. 467 ss.; F. DI CIOMMO, *La buona fede correttiva di regole contrattuali*,in *Contratti*, 2000,p. 1111 ss.

[28] R. MORTIER, H. HADDADI, T. HENDERSON, D. MCAULEY E J. CROWCROFTL, *Human Data Interaction: The Human Face of the Data-Driven Society, in https:// ssrn.com/abstract=2508051*, in original in the text "*the capability of individuals to autonomously understand data and analytics algorithms, with a concrete comprehension of methods and data used*"; G. MALGIERI E G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, VII - IV, 2017, p. 249.

[29] G. MALGIERI E G. COMANDÈ, *op. cit*., E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualita` dei dati e leggibilita` dell'algoritmo nella cornice della responsible research and innovation*, in *Le Nuove Leggi Civili Commentate* V, 2018.

courts have acknowledged that there is a right to a real understanding by individuals who are subject to automated processing in the individual decisions affecting them[30].

All this being said, the elements highlighted so far allow us to advance the first considerations in the Bologna specific case, from which this work has taken its cue.

If indeed, as highlighted, it is necessary to apply to the contract between user and social the consumer discipline, and that requires particular clarity (if not a real obligation of knowability), the professional conduct of the closure of the profile appears particularly objectionable, even as outlined by the terms of agreement of the social network in question.

These ones (section 4.2) highlight the possibility of closing the account, but in a very general way; for example, it will be possible to suspend or close an account for the "(un)truthfulness of the contents". It seems obvious that the obligation of transparency, legibility and especially information on the automated procedure is not, in this way, complied with, since the user cannot know the decision-making mechanism that leads the automated system to retain its contents "truthful" or not.

Nor, according to the terms of use, the social has to warn the user, reserving Facebook not to proceed with notice if this may expose him to "legal liability" (paragraph 4.2); the formula, as is clear, is of such impact that it is considered to generate a total discretion of the social network with regard to the notice.

On the basis of these considerations, the Bologna Court has - according to this writer, correctly - considered more than well-founded the requirements to recognize a responsibility of the digital platform. Indeed, non-material damage can certainly be recognized based on the violation of the digital identity of the subject, in the broad sense, and in particular in his freedom of expression of thought, specifically within the network.

A lot of elements that have been discussed so far are leading this evaluation, but primarily the obligation of "strengthened" information which the consumer-user is undoubtedly the beneficiary of. Especially in the present case, this right is largely ignored by the digital platform, but not only that.

In fact, the professional has made use of such vague and general contractual conditions that it is substantially useless for information purposes, as well as the lack of notice to the user, a further symptom of the condition of subjection that the professional imposes

---

[30] In particular, the Italian Administrative Supreme Court, or "Consiglio di Stato", with the pronunciation Sez. VI, 8 aprile 2019, n. 2270 - Pres. Carbone - Est. Lamberti - *M.A. ed altri c. Ministero dell'Istruzione dell'Università e della Ricerca ed altri*.

Once established that the algorithm must be considered an administrative act it should be comprehensible to those who are affected by it, like it is for any other administrative choice. In the Italian version "*la piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico deve essere conoscibile* […] *in tutti i suoi aspetti*". Consider also V. CANALINI, *L'algoritmo "come atto amministrativo"* in *Giornale di Diritto Amministrativo*, VI, 2019; Corte di cassazione, Ord. 24 marzo- 25 maggio 2021 n. 14381 Pres. Genovese; Rel. Terrusi; Pm - difforme - Cardino in *La Guida al Diritto*, XXIV, 2021, p. 70 ss.

on its digital consumers-users, even not deserving, according to the first one, a right to notification about the closure of their social profile.

VI. FURTHER CONSIDERATIONS

So far, efforts have been made to face the complexity of the legal aspects of the case, which has recognized the existence of non-patrimonial damage on the basis of the harm to an aspect of the digital identity of the subject, in particular the social network activity of the consumer part. Moreover, the professional part is one of unquestionable strength not only under an economic point of view but also technological, and without even warning he has compromised the online activity of an user-consumer.

The reasoning so far proposed deserves further analysis, trying to question - *pro futuro* - what might happen in two different circumstances.

The first relates to the case where the conduct so far analyzed will be repeated not in sporadic cases, but rather to an increasing number of users; in this case, it seems conceivable that the institution of unfair commercial practices could be used.

The second hypothesis is that of forced closures of digital profiles by digital platforms not in relation to users-consumers but rather to companies or firms that have a page within the platforms themselves, with a further distinction between public enforcement and private enforcement.

1. Unfair commercial practices within the network

The unfair commercial practices[31] found its origin in the European regulations (Directive 29/2005, transposed in Italy with the d.lgs. 206/2005) and has the aim of generating a sanction against those firms which impose themselves on the market in such a way as to mislead the consumer or which, in any case, influences the “average” consumer accordingly[32].

[31] C. CAMARDI, *Pratiche commerciali scorrette e invalidità*, in *Obbl. e contr*., 2010, VI, p. 408 ss.; C. CAMARDI, *La protezione dei consumatori tra diritto civile e regolazione del mercato*. *A proposito dei recenti interventi sul codice del consumo*, in J*us Civile*, V, 2013, p. 305 ss.; E. BATTELLI, *Codice del consumo, codice civile e codici di settore: un rapporto non meramente di specialità*, in *Europa e Diritto Privato*, II, 2016, p. 425 ss.; G. DE CRISTOFARO, *La nozione generale di pratica commerciale “scorretta”, in Pratiche commerciali scorrette e codice del consumo*, 2008, p. 143 ss.; A. NOBILE, *Le tutele civilistiche avverso le pratiche commerciali scorrette*, in *Contr. Impr. Europa*, 2014, pp. 180-199; A. FACHECHI, *Pratiche commerciali scorrette e (apparente) “gap” normativo: il “sistema” dei rimedi negoziali*, in *Studium iuris*, 2015, I, p. 181 ss.; A. P. SEMINARA, *La tutela civilistica del consumatore di fronte alle pratiche commerciali scorrette*, in *I contratti*, VI, 2018 p. 689 e ss.

[32] C. CAMARDI, *La protezione dei consumatori tra diritto civile e regolazione del mercato*. *A proposito dei recenti interventi sul codice del consumo*, in J*us Civile*, V, 2013, p. 305 ss.

The aim of the institute is therefore to generate a legal response to the unfairness and negative effects of a competitive market economy[33]. The need for intervention (the competence of which lies with the Italian Antitrust, or AGCM) responds to an increasingly strong refinement regarding the pervasive techniques of operators within the market.

As known, the institute was created to protect consumers and - therefore - the first question to be asked is the possibility of applying the sanctions that the institute provides also in the digital context, in particular regarding social networks.

The answer is yes. Not only because the Authority has been able to clarify on several occasions the applicability of the unfair commercial practices to the digital context[34], but also for the reason above with respect to the debate on the relationship between user and social networks. In fact, even according to the recent Directive 770/2019, it does not seem doubtful the applicability of consumer discipline (if not the full recognition of consumer status) to the user of the digital platform, including the regulation of unfair commercial practices.

The use of such a strong remedy allows to intervene where the consumer (or the consumer alone) could not: to impose significant fines on companies of great economic strength; between 2017 and mid-2021, the sanctions imposed by the Italian Antitrust Authority alone on Facebook amount to more than 20,000,000.00 euro[35], whereas the compensation for the damage recognized in the Bolognese case of March 2021, treated at the beginning of this work, recognized a few thousand euros to the user.

A difference undoubtedly remarkable against the patrimonial value of the society called to answer of the conduct (and the conducts) in examination, especially for a firm today estimated at approximately 1.000.000,00 billion dollars (about half of Italian GDP; however, Facebook is not an isolated case, since it is not far from the estimated value of the other “over-the-top” firms in the US, like Apple, Amazon, Alphabet[36]).

Apart from the obvious difference in imposing significant sanctions on these companies, it seems important, nonetheless, to question the effectiveness of sanctions even of this amount, according to the economic successes that these companies continue - in any case - to obtain.

---

[33] A. P. SEMINARA, 2018, p. 689 e ss.

[34] Among others consider the “Juice Plus” case, entirely reported on the authority web site, *ttps://www.agcm.it/dotcmsdoc/allegati-news/PS11050_scorr-sanz_omi.pdf.*, Consider also the pronunciation of the authority “Agcm 1aprile 2015, n. 25411”, link *https://www.agcm.it/dettaglio-ricerca?id=e9eb44a7-8151-4195-89aa-c71c30a6473.* More recently, a pronunciation of the Rome administrative Court has rejected the appeal of Facebook against the Antitrust Authority in this very topic (pronunciation 261/2020).

[35] Consider on this very point the pronunciation of the Authority 26597/2017, 27432/2018 and 28562/2021

[36] Data referred to the second quarter of the 2011.

2. Protecting the digital profile of companies

The issue of the protection of the digital identity of the user has been addressed, as for the undoubted advantages that exist in recognizing the typical protection of the consumer. At this point of the discussion, however, we must focus on a final aspect, that of the legal aspects linked to the eventual closure of the digital profile of the companies.

Commercial activities, in fact, often use digital (in general) and social (in particular) platforms for advertising or commercial information.

At first sight, the problem seems not to be relevant, since commercial companies must be considered professionals (as well as the digital platform) and it is their burden to sign for contractual agreements (even without space to bargain, as in the case of Facebook or others social network) that they found convenient.

In any case it will be their choice to use the ordinary civil law remedies in the event of an unlawful act, for example when a profile is closed without any justifications, according the contractual conditions, asking in particular for pecuniary compensation.

However, a different perspective seems necessary. It has already been mentioned, in fact, the economic strength of the companies involved, and this has prompted the Doctrine, the Antitrust Authority and the Jurisprudence to question themselves about a different reading of the phenomenon, framing it in the case of the Abuse of Dominant Position[37].

In fact, on the basis of this subject (regulated in Italy by L. 287/90, and in the European Union in general by art. 3 and art. 102 TFEU) the activity of the companies cannot be censured (only) for their situation of domination within a given market context, but rather to exploit this position, causing harm to consumers or obstacles to the exercise of the commercial activity of competitors, even if in a potential way or in determining - thanks to their contractual force - the signing of contracts that generate an excessive imbalance of rights and obligations also taking into account the possibility of finding “satisfactory alternatives on the market” (L. 192/1998, art. 9).

---

[37] R. MORO VISCONTI, *Danno antitrust e piattaforme digitali*, in *Il Diritto Industriale*, I, 2021, p. 5 ss.; P. SPAGNOLETTI - A. RESCA - G. LEE, *A design theory for digital platforms supporting online communities: a multiple case study*, in *Journal of Information Technology*, 2015, XXX, IV, pp. 364-380; R. MORO VISCONTI, T*he Valuation of Digital Intangibles. Technology, Marketing and Internet,* PALGRAVE, MACMILLAN, 2020; *Antitrust Source (Apr. 2015), Online*, University of Tennessee Legal Studies Research Paper No. 269, 2020, in *https://ssrn. com/abstract=2600051*. In particular about algorithms and antitrust A.M. GAMBINO - M. MANZI, I*ntelligenza Artificiale e tutela della concorrenza*, in *Giur. it.*, 2019, p. 1744; A.P. GRUNES - M.E. STUCKE, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data* (April 28, 2015).

In general on this topic C. OSTI, *Diritto della concorrenza*, Bologna, 2007; A. PERA, *Concorrenza e antitrust*, Bologna, 2009; L. PROSPERETTI - M. SIRAGUSA - M. BERETTA - M. MERINI, *Economia e diritto antitrust,* Roma, 2006; consider also the prunciations Cons. Stato, 2631/2021 e Cons. Stato 3851/2021.

In these cases, the Antitrust Authority can intervene if it detects risks or facts that lead to distortions of the market.

Apart from the patrimonialization of Facebook, the number of users of the platform, as well as the segmentation of the target of reference leave little doubt on the satisfaction of these requirements. In fact, if a company (perhaps of modest or very modest size) wanted to advertise itself online (a necessity even more felt in the past months, marked by the pandemic context) would have little choice.

The Facebook platform has absolute records of subscribers compared to the potential catchment area, followed by a short distance by Instagram (which belongs to the same holding company): the registered users are close to three billion, for about 1.84 billion monthly access[38], with a number of users in Italy alone of 38 million and two hundred thousand, with about 80 million registered companies[39].

Even more drastic is the situation of defining the consumer market of reference: it appears in fact essential for the launch of an effective sales plan to define the target of a product or a service.

However, even more so in certain anagraphic cohorts an effective advertising campaign seems to be unable to escape from the well-known social platform, since 98% of Italian people between 30 and 35 years and 78% between 36 and 45 years are registered on Facebook[40] (younger people seem to prefer, unlike the other platform of Facebook Inc., Instagram, where 71% is under the age of 35).

In the European context social networks seem even more appreciated, since the social network participation has significantly increased in the last ten years, while Italy is one of the least European country for social network use[41].

In practice, the commercial strength of the platform makes it very difficult (if not in concrete impracticable) to find a viable alternative in terms of commercial channel, thereby delineating a market concentration that excellently satisfies the Antitrust canons for the

[38] Data from *emarketer*, link *https://www.emarketer.com.*

[39] Data from the Vincos observatory based on Nielsen data, link *https://vincos.it/osservatorio-facebook/.*

[40] Data from *emarketer*, link *https://www.emarketer.com.*

[41] In particular, according to Eurostat, in the EU 54% of people aged 16-74 participated in social networks in 2019 in the last 3 months prior to the survey. The EU's social network participation rate has steadily increased since the beginning of the data collection (36% in 2011).

In fact, Among EU Member States, the social network participation rate was highest in Denmark (81%), ahead of Belgium (76%), Cyprus and Sweden (both 72%) and Malta (71%). At the opposite end of the scale, this share was below 50% in two Member States: France and Italy (both 42%). More on this topic in the Eurostat site, link: *https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20200630-2*.

emergence of a dominant position, clearly abused where the contractual clauses allow the unilateral closure of the profile without prior notice or explicit reason.

DIGITAL DIVIDE AS AN INEQUALITY FACTOR. A STUDY FOR THE DIGITAL FUTURE IN THE PACIFIC REGION

Por

AKIHISA HIRANO / VICTORIA GRANDA
University of Valencia. Japanese business developer based in Valencia, specialize in Human Rights and New Technologies / University of Valencia. Ecuadorian lawyer specialize in Digital rights, New Technologies, and Data protection in Latin America region and EU

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

ABSTRACT: This paper studies how a digital divide as an inequality factor between regions has an impact on job opportunities in a globalized and digitalized world. In doing so, first of all, we analyze existing factors behind a digital divide taking place, which helps us get a better understanding of what kinds of problems we are facing. Secondly, we are going to look into legal and political countermeasures against digital divide in the Pacific Region. Finally, we are going to evaluate those measures to see if they contribute to decreasing inequality caused by digital divide in practice.

KEYWORDS: digital divide, digital gap, inequality, digitalization and innovation, human rights, access to internet, artificial intelligence, Fourth Industrial Revolution.

SUMMARY: I. INTRODUCTION. II. FOURTH INDUSTRIAL REVOLUTION AND DIGITAL DIVIDE. 2.1. The development of Artificial Intelligence, Internet of Things, 5G and inequalities for individuals and society. III. IMPACTS ON LABOUR MARKET: WORKFORCES AND PROFESSIONAL. 3.1. Polarization in the labour market: a complex future. IV. EDUCATION AND SKILLS FOR A DIGITALIZED MARKET. 4.1. Digital literacy and education systems to narrowing the digital gap: Japan legal framework. V. CONCLUSION - DIGITAL DIVIDE AND THE DIGITAL FUTURE IN THE PACIFIC REGION. VI. References and Bibliography.

LA BRECHA DIGITAL COMO FACTOR DE DESIGUALDAD. UN ESTUDIO PARA EL FUTURO DIGITAL EN LA REGIÓN DEL PACÍFICO

RESUMEN: Este trabajo estudia cómo una brecha digital, en tanto que factor de desigualdad entre regiones, tiene un impacto en las oportunidades de empleo en un mundo globalizado y digitalizado. Al hacerlo, en primer lugar, analizamos los factores existentes detrás de una brecha digital, lo que nos ayuda a comprender mejor qué tipo de problemas enfrentamos. En segundo lugar, vamos a examinar las contramedidas jurídicas y políticas contra la brecha digital en la región del Pacífico. Finalmente, vamos a evaluar esas medidas para ver si contribuyen a disminuir la desigualdad causada por la brecha digital en la práctica.

PALABRAS CLAVE: brecha digital, salto digital, desigualdad, digitalización e innovación, derechos humanos, acceso a internet, inteligencia artificial, cuarta revolución industrial.

I. INTRODUCTION

The theme of digitalization is likely to be focused on its benefits and advantages, which surely contributes to our society and our daily life. There is no wonder that new technologies will facilitate and advance the process of what we do on a daily basis. History has witnessed the First Industrial Revolution and now we are in the middle of this emerging Fourth Industrial Revolution along with artificial intelligence technology - AI, machine learning, deep learning, etc. We are moving forward the era of automated society connected with AI. Meanwhile, there are still some countries where more than half of citizens do not have access to the internet, a digital divide in a traditional sense, which deals with the access to the internet, has been recognized as an issue since the early XXI century.

However, we have been seeing something unprecedented for the past years with a swarming introduction of digitalization into our society, which is shedding a light on another aspect and evolution in a digital divide. As digitalization evolves, a digital divide is transforming by itself, which results in making a digital divide wider. Especially in developing countries in the Pacific Region[1] such as the islands of the Asia-Pacific cost, Papua New Guinea, Solomon Islands, but also in other latitudes of the Pacific Ocean, as Colombia, Perú or Ecuador, where they are still facing a digital divide. In this sense, it is only logical to intend to understand and replicate what developed countries in the same region have done to overcome these issues.

On the other hand, Japan has already established a broadband infrastructure with a high-speed internet all around Japan. The Japanese government drafted a plan to adopt a STEAM education and AI literacy education as mandatory subjects in the public educational system. The 5G network is the foundation that enables the implementation of digitalization to be viable and sustainable. With the absence of the 5G network, the advancement of the Fourth Industrial Revolution surely will leave developing countries fossilized and stuck without much accessibility in the process of digitalization.

The core idea of the Fourth Industrial Revolution lies in automation of processes where people conventionally work and subsequently the automation becomes, what we call, innovation because these systems of AI technology and the robots' function instead of people much more efficiently.

For to naming some operative examples: 1. Robot Advisors in the financial industry advise you what to buy and sell financial products based on mathematics assessment

[1] For the purpose of this study, we are referring to the Pacific Region to the countries in the Asia-Pacific and those in America continent as well, which are on the coast of the Eastern Pacific Ocean.

evaluation systems through algorithms by substituting human financial advisors. Another example is, the first Robot's lawyer in the world, "DoNotPay", which originally started to offer legal services concerning how to appeal parking tickets through AI system in the UK. 2. Applicant tracking system (ATS), an AI system that Amazon adopted in the recruiting process to pre-screen applicants. 3. Bounsel, a valencian start-up, is developing an automatic labour contract system.

These are all examples of automation, which undoubtedly have an enormous impact on the labour market meanwhile the 5G network is a necessity to materialize automation. Therefore, the labour markets have been requiring numerous AI experts, programmers, and modelers in every industry for the past years. However, with only 1 woman in 5 people working in the industry today[2], it is evident that the tech industry is male dominated. This may play out as an inequality factor as a glass ceiling effect for female's job opportunities and affect the gender gap in income. On another aspect, every worker tends to be required to possess a certain knowledge concerning AI.

However, the polarization, which separates 'brains' and 'hands', may be accelerating through automation. Theoretically, automation boosts to reduce the intermediary tasks as shown in the examples of the previous paragraph. In the case of the Amazon recruiting process, it requires workers who design algorithms to evaluate resumes and operators who maintain the system. In all likelihood, the polarization reduces the intermediary jobs and contributes to cementing the structure of the separation in highly skilled workers and low skilled workers who look after basic tasks. Being confronted with these findings, it is evidently crucial for governments to take effective measures to decrease potential inequality risks derived from a digital divide with establishment of legal framework and support on a national, regional, and global scale.

II. FOURTH INDUSTRIAL REVOLUTION AND DIGITAL DIVIDE

Globalization and the dawn of disruptive technologies paved the path to the Fourth Industrial Revolution, which transformed mainly the economy, production, the acquisition of property and services, and of course us as humankind. In doing so, we have seen unprecedented realities, new forms of employment, even new terms; nowadays we discuss LegalTech, Gig Economy, Blockchain, and Smart contracts. Undoubtedly, with the implementation of the 5G network, the growing of Internet of Things - IoT, and the developing use of AI, it is sufficient for us to say that the future of full digitalization is becoming a reality.

[2] Women in Tech, *Why we exist.* Available in: https://women-in-tech.org/context/. Last access: 14-09-2021.

The Fourth Industrial Revolution surely has numerous benefits for the societies, the industries, which range from ensuring the capacity to connect millions of people through the digital network, to optimizing the efficiency of the organizations, and to reaching innovation. In this context, it is usually pointed that only disruptive technologies allow this purpose, yet innovation can be accomplished by improving and making any kind of changes thus resulting in new paradigms and scenarios where innovation happen. It takes society enormous efforts to make a paradigm shift of full digitalization and it is not easy to adopt new rhythm and methods against new circumstances. The resistance to changes against it, however, is the outcome of human nature.

Industries and markets can take advantage of public trust to improve and promote life's quality to individuals by accepting better opportunities through innovation, mostly in developed countries and similar regions. Nonetheless, this scenario cannot be applied to developing regions as this new technology era increases pre-existing inequalities, raising polarization and fragmentation of society, labour markets and professionals on larger scales.

Having said that, although in some regions are more prepared to adopt the Fourth Industrial Revolutions than others, the lack of knowledge on what, who and how the impact this transition has, we must be open to debating, analyzing and to imposing this questions through multiple points of views, therefore, it is crucial to make sure we - scholars, political actors and general public, understand sufficiently in order to constrain negative impacts on human rights, inequalities factors and life's quality.

Digital divide has been a serious issue even before the Fourth Industrial Revolution not only in developing countries. In 2011, the Ministry of Internal Affairs and Communications of Japan raised the question regarding the digital divide through the annual White Paper Report. In this issue, it was suggested that there was a huge difference in income caused by the digital divide between those who have more access to the internet in comparison with those who have not. It shows that Japanese citizens with an annual income of more than 15 million JPY utilizes the internet by 85.3% On the other hand, one with an annual income of less than 2 million JPY utilizes the internet by 50.5%. The 2020 report deals with the viable future with the implementation of 5G in the Reiwa Era[3]. The 5G service was initiated in 2020 by those providers with the target of 160 million users by 2025. The establishment of high-speed internet has been a main focus in the IoT strategy in Japan.

However, in 2016, The World Bank issued Digital Dividends as a main challenge in its annual report. It argues to increase connectivity as a premise for the 5g Infrastructure and

[3] MIC ICT. *White Paper 2020, Information and Communication in Japan 2020 (summary,* Ministry of Internal Affairs and Communications, Tokyo, 2020, p. 3.

to enhance the implementation with analog complements needs to be considered carefully[4]. In other words, it is crucial to make the internet accessible, affordable, open, and safe to diminish a digital divide at an initial stage before keeping up with the Fourth Industrial Revolution. Simultaneously, in order to materialize it, legal regulations are necessary to legitimize this measure so that everyone can make full use of opportunities to have access to the internet. The digital divide, in a conventional sense, can be defined as an asymmetry between access to digital infrastructure and services between individuals.

A digital divide can be mainly classified into three segments. The first one is a domestic regional difference, which suggests a difference caused by a region within a country. The second one is an individual difference caused by a physical condition and socio-economic condition such as gender, age, academic background. Lastly, the third is an international difference, which indicates a difference among countries. The 4.0 industry has been accelerating and boosting the effect of those mentioned asymmetries, or as we will call: inequality factor.

2.1. The development of Artificial Intelligence, Internet of Things, 5G and inequalities for individuals and society

In the Pacific Region, the Fourth Industrial Revolution raised the question regarding asymmetry of power between citizens and government. China, for example, issued a massive AI investment strategy in 2017 - Plan for the Development of New Generation Artificial Intelligence or 新一代人工智能发展规[5], which allow to establish surveillance state using AI systems as a formidable instrument to control people. Thereby, in 2020 with the COVI-19 pandemic situation, China took the opportunity to justify monitoring citizens in China and Hong Kong such as the development of the APPs to track people through drones and video vigilance[6].

In this sense for example, through AI systems enabled themselves to identify those not wearing facemasks in public and detect fevers. Seemingly, COVID-19 boosted the investment into surveillance technologies with a legitimate reason. China's massive surveillance results in asymmetry of power between citizens and governments. This example clarifies how asymmetry became or developed on an inequality issue, as we will

[4] World Bank, *World Development Report 2016: Digital Dividends*, World Bank Publications, Washington D.C, 2016, p. 2

[5] China Innovation Funding, *State Council's Plan for the Development of New Generation Artificial Intelligence.* Available in: https://chinainnovationfunding.eu/dt_testimonials/state-councils-plan-for-the-development-of-new-generation-artificial-intelligence/. Last access: 13-09-2021.

[6] PETERSON, D.: "Designing Alternatives to China's Repressive Surveillance State", *CSET Policy Brief,* Georgetown's Walsh School of Foreign Service, Washington D.C, 2020, p. 10.

explain. The exponential development of AI is apt to encompass enormous disadvantages, which might signify an evolving process, mainly that is, a technological divide that would augment more than present because of scarcity of institutional support in politics and legal framework that guarantee better competency but increase in lack of privacy, transparency, and other variety of aspects.

Moreover, not only sophisticated, and complex technology as AI systems represent risks, since mobile phone and mobile devices are more likely to be accessible to people than clean water. Mobile devices are often the only way to access Internet in a low and middle-income countries. According to Global System for Mobile Communications Associations - GSMA's report *The State of Mobile Internet Connectivity Report 2021*, despite the COVID-19 pandemic, more than half of the world's population is now using the mobile internet. Mobile internet usage translates to just over 4 billion connected people[7]. Although it seems to be detected two trends to work on to bridge the Digital Divide: coverage and usage gap.

Coverage gap is related to connectivity, commonly referred to people without access to mobile internet services. As Internet's access is still a big challenge that increase digital dividends, especially, since it was launched the 5G com-antennas. Internet and 5G are pointed as enablers of the fourth revolution industry, as it enhances the quality of communication and its speed through the internet. It has a huge impact on every part of our life considering to connect people to industries and markets at a rapid rate flawlessly, and making possible smart city viable but also help to drive rural connectivity with high-speed internet.

In Latin America around 300 million people may not be able to connect to the internet and it is estimated to increase up to 53 million users, that is, 7% connection of 5G. This is a very low rate, as we compare with the forecasts from other regions, Asia Pacific Region 11% - China 47% and Japan 56%-, Europe within 34%, and North America 48% in the projection[8]. A report from CAF -Development Bank of Latin America/ Andean Development Bank, if each region decreases the digital divide by 2030, it will bear a significant impact on the productivity up to 3% on the GDP annual, USD 700.000 million of growth, creating more than 400.000 jobs[9]. Nevertheless, to achieve these projections,

---

[7] GSMA. *Over Half World's Population Now Using Mobile Internet.* Available in: https://www.gsma.com/newsroom/press-release/over-half-worlds-population-now-using-mobile-internet/. Last access: 12-09-2021.

[8] GSMA, *The mobile Economy in Latin America 2020.* Available in: https://www.gsma.com/mobileeconomy/latam/. Last access: 14-09-2021.

[9] CAF, *Digital Transformation for 21st-Century Latin America*. Available in: https://www.caf.com/en/knowledge/views/2020/02/digital-transformation-for-21st-century-latin-america/. Last access: 14-09-2021.

it requires the improvement of public policies, for example, tax incentives for technological/digital transformation.

Usage gap, on the other hand, is a bigger challenge. According to GSMA in 2020, 3.4 billion people - 43% world's population, live in areas that are already covered by mobile broadband network but are not using it, this might find its reasons in the lack of affordability or lack of awareness as well. Broadband internet affordability since the dawn of the internet issues has increased due to the economic impact of the pandemic situation in low- and middle-income population and countries.

This results in that all-ages students, young professionals, and unemployed people in risk have not been available to exercise fundamental rights - as Internet works as an element to enable fundamental rights in the legal framework of Information Society and Media such as education, information and communication, worthy occupation, mental health and others -, and the development of essential skills as individuals. For example, during the lockdown due to the pandemic situation, people with mobile internet access were not only able to stay connected with family but access to virtual/on-line education, conduct business and remote working, or to have access to critical information and services.

The COVID-19 pandemic gave us a wakeup call for us to realize the necessity of digitalization in various areas, from education to the labor market. In the aftermath of the COVID-19, nor remote work is no longer as rare as before neither e-learning. The implications were very influential, it revealed the importance of having a digital infrastructure for this new reality: telework, e-commerce, delivery, cashless payment systems and virtual or online classes. During the pandemic, organizations that had already started a digital transformation established a better strategy for the implementation of the digitalization and performed better during the pandemic.

This phenomenon applies to governments, for example, the countermeasure and health management against the pandemic had a faster and therefore more efficient tracking response for infected cases where optimal network/internet connectivity already existed. Thus, the speed of management response is related to connectivity, and so to access to the Internet. There are plenty of countries in the Pacific Region where they do not even have sufficient internet access, especially, one of those island countries such as New Caledonia, Papua New Guinea, Solomon Islands, etc[10]. Therefore, a digital divide caused by the fourth revolution leaves them behind so far in this transition of digitalization because those countries are still in the previous phase to enhance the accessibility of the internet, which is the base of the path to the digitized world.

[10] GSMA, *Mobile Internet Connectivity 2021 East Asia and Pacific Connected Society Key Trends*. Available in: https://www.mobileconnectivityindex.com/. Last access: 13-09-2021.

III. IMPACTS ON LABOUR MARKET: WORKFORCES AND PROFESSIONALS

As new technologies dawn and old devices become obsolete, workers and professionals need to acquire new skills to adjust themselves to the changing labour market. New technologies as Big Data, Internet of Things, Blockchain or Artificial Intelligence that have been mentioned and developed over the course of the Fourth Industrial Revolution, and have a driving force to transform workplaces, consumer habits, logistics and supply chain, among other business patterns; surely, the conventional industries tend to vanish or to be reduced if they do not prepare. In the context of digitalization, it is common to assume that some jobs could possibly disappear with the help of automation, usually pointed as one of the main challenge and concerns.

By and large, following the report from the World Bank, the impacts of digitalization on the labour market are positive on employment and income. The innovation of digitalization is likely to create more jobs in conventional industries and new jobs opportunities in new industries. It also helps to enhance productivity because of the nature of the digitalization, which enables companies to gain more profits and workers can benefit from those profits. The digitalization can lower the cost of products and services by nature, which enables the market to produce new types of products and services. Even though digitalization is causing a positive effect on the whole, regarding the poorer the other data shows that they do not benefit from the digital sector nor the sector where digitalization is applied.

In 2013, Oxford University's researchers and professor Carl Benedikt Frey and Michael A. Osborne published a study of the impact of automation in the US labour market. It covered a wide range of 702 respective occupations of different characteristics with a view to defining risks and probabilities of replacement of human workers with machines in the context of automation. Using the base of the data O*NET - an online service developed by the US Labour Department, which, in compliance with a series of standardized and measurable indicators, defines the characteristics of each labour occupation and includes each description of 277 requirements in capacity for each role, they completed this study with the data of employment for proportional occupations derived from the US Bureaus of Labor Statistics. By using some algorithm, it estimated that 47% of the occupations would be at risk in the US.

Following this study, the World Bank adopted this same model in 2016 for a larger application, it was reported that there were major risks recognized in developing countries and approximately, a two of thirds of occupations are susceptible of automation[11]. In this

[11] SOLAR CAYÓN, J. *La inteligencia artificial jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*. 1ª ed., Aranzadi, 2019, p. RB-1.3.

context, in 2015 was launched a study of Nomura Research Institute in 2015, which mainly deals with social implications caused by adopting AI in Japan, according with it within 20 years 49% of the labour force is estimated to be replaced by technically AI or AI robots[12].

Most jobs and work that do not require special skills and knowledge and the ones that can be programmed easily without any compelling process are replaceable by AI. On the other hand, it reports that the jobs and work that require certain creativity dealing with abstract concepts, negotiations, persuasions, and high demanding manpower services are not likely to be replaceable. Facing all the potential realities and changes in the job market, it is necessary to look into an education system to cope with an evolving job market.

Name of Study	**Impacts on the Labour Market**
The Future of Employment, Frey & Osborne (2013)	47% of the jobs in the US are replaceable (the UK 35%).
NRI Report (2015)	49% of the jobs in Japan are replaceable.
The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis (2016)	There are only 9% of work at risk. It suggests that many other projections from other related studies are likely to be overestimated by number.
IoT, Big Data, AI impact on employment and labour (Japanese Ministry of Health, Labour and Welfare) (2017)	It is necessary to look into this reality first and a drastic change will not be expected in the labour market.
Latin American Economic Outlook 2020: Digital Transformation for Building Back Better (2020)	With the economic crisis generated by the pandemic, job loss could be massive. Unemployment in LAC could rise to 13.5% at the end of 2020.

As we can see from the table, the most recent studies show more favorable results, in terms of the risks in replacement of work, than those of Frey and Osborne's models; that is, applying tasks instead of occupations, such as the study by M. Arntz., T. Gregory, and

[12] NITTO, H., TANIYAMA, D. and INAGAKI, H.: "Social Acceptance and Impact of Robots and Artificial Intelligence - Findings of Survey in Japan, the U.S. and Germany", *NRI Papers*, nº 211, 2017, p. 2.

U. Zierahn[13], in coordination with the OECD, published in the same year as the World Bank study, the risk of automation in developing countries on average indicates 9%. Besides, the capacity of the investment of technological resources in each State is a determining factor, both in automation and in the education and training of workers.

3.1. Polarization in the labour market: a complex future

An enormous shift to automation has a direct effect on the labour market: polarization. Polarization causes the demand for middle-level workers to leave the job markets, for example, administrative assistants, while increasing jobs with the high cognitive ability with non-routine interpersonal skills and low cognitive skills with non-routine manual skills, e.g., university students and professors or cleaning staff. Automation and digitization encourage change in the structure of the process in work. However, it affects jobs that require intermediate skills because they are becoming less and less necessary as automation advances more and more. This trend will only be accentuated in the coming years. Although, the principal goal is not automation, but innovation.

Innovation is the phenomenon caused by modifying certain elements; the results and processes are new and improved. Therefore, automation in the labor market is likely to result in innovation in organizational structures. For instance, the emergence of start-ups and SMEs in the tech industry is proof of that; physical spaces, e.g., online work, the workplace is the same where we are supposed to rest; new services and products, v.g sharing and app-based-economy uber, glovo and deliveroo.

According to Vice President for LAC Region World Bank, Felipe Jaramillo, the pandemic had a huge impact on Latin America: with a projection of 7.9% decline in regional GDP in 2020, 25 million jobs could disappear[14]. In Ecuador, according to OECD[15], SMEs occupy 60% of employment in the country[16]. Hereto, these types of companies have fewer resources - economic and human capital - to face possible losses in profit. Thus, approximately 35% of jobs which were highly impacted by the crisis of the pandemic are commerce, manufacturing, and the tourism/hospitality sector, while jobs

[13] ARNTZ, M., GREGORY, T. y ZIERAHN, U.: "The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis", *OECD Social, Employment and Migration Working Papers*, nº 189, OECD Publishing, Paris, 2016.

[14] JARAMILLO, C. F.: *Closing the digital gap to end poverty in Latin America and the Caribbean.* Available in: https://blogs.worldbank.org/latinamerica/closing-digital-gap-end-poverty-latin-america-and-caribbean. Last access: 13-09-2021.

[15] OECD.: *Latin American Economic Outlook 2020.* Available in: https://www.oecd.org/dev/latin-american-economic-outlook-20725140.htm. Last access: 13-09-2021.

[16] OCDE. "Social impact of COVID-19 in Ecuador: challenge and responses", *Making Development Happen*, Vol. 4, 2020. p. 8.

related to transportation and communications have had a medium average impact with 6.7% occupation of the labor market.

Thus, with COVID-19, the other side of digitization has become evident. The digital divide in the labor market increases inequality by impairing the quality of employability and labor rights. For example, Chile, Peru, and Ecuador, had to accelerate labor regulation regarding remote work either because the figure did not exist in their legal framework - as it was the case of the Chilean labor act, or they contained legal loopholes that made it impossible to use it, as in the Peruvian legislation. After a few months later after the pandemic outbreak, Ecuador published the Organic Law of Humanitarian Support to Combat the Health Crisis derived from COVID-19 regulated teleworking and the right to digital disconnection[17].

Despite this, 154 complaints of workplace harassment were filed in the Unified Labor System, between March 16th and October 7th, 2020. Remote working became mandatory except for essential jobs, most complaints shifted from work related to work overtime, which is approximately 15 working hours per day but receiving the amount of payment equivalent of 6 working hours. However, neither pandemic or digital divide cannot lead to a regression in fundamental rights, working conditions, or quality of life.

In Japan, the COVID-19 also impacted the labour market in a tremendous manner. Regarding home office, in terms of productivity of work, employers and employees both are more favorable for working in the office than home office, based on the questionnaire performed in June 2020. Only 3.9% of employees and 1.2% of employers answered that a home office is more productive, compared with the situation in the US, which indicated that 41.2% of employees answered that a home office is more productive. Currently, working remotely is still not common in Japan, and it is expected that employees will be able to return to work in the same condition in their habitual workplaces.

On the other hand, in Japan there are no legislation, act or regulation that contemplates the right to disconnect, so it is rather being promoted voluntarily by companies. During the pandemic, there were plenty of complaints reported to labor unions where some companies did not allow temporary workers to work remotely while full time permanent workers were. Some cases were elevated to trials because employees were dismissed because of their conflict with companies. Those companies explained that it was owing to the protection of confidential information, and it was not sufficient to offer a telework environment to all employees. We can recognize an inequality in terms of the working condition based on the type of contracts.

[17] Digital disconnection is the action of disconnecting from electronic devices.

However, digital divide in workplaces functions as a driven force for other factors of inequality - e.g., lacking gender perspective and glass ceiling, and in a broad sense, biases issues, and inequity - thus gender, race, age or level/access of education. But digital landscape is in all likelihood to be urgent in needs of capable workforce and professionals willing to take advantage of the interdisciplinary nature of the Fourth Industrial Revolution in order to succeed in innovation. Therefore, an analysis of these assets is essential for a better understanding, and moreover to get a panoramic view of how the Pacific Region is dealing with these new scenarios.

IV. EDUCATION AND SKILLS FOR A DIGITALIZED MARKET

Innovation, as we have mentioned, is the main purpose of the Fourth Industrial Revolution. Yet, how we achieve innovation is the real question, as it is a wide concept. No wonder why many organizations and institutions - publics, and privates- are willing to perform joint efforts by implementing a variety of strategies and initiatives to estimate the impact of new technologies on markets and preparing human resources - professionals and labour forces.

According to the AI Experience 2021 report - a collaboration between CAF, Telefónica, Microsoft and C4IR.CO, a center affiliated with the World Economic Forum for the Fourth Industrial Revolution in Colombia, it was possible to identify three gaps that organizations would face in order to accomplish automatization and the implementation of AI solutions: organizational capacity gap, motivation of the workforce and the preparation of human resources.[18]

Regarding this paper, we are going to focus primarily on the two first issues. Organizational capacity gap refers to a significant asymmetry or disparity between an organization's goals and objectives v. its actual or potential ability to achieve its vision and mission. The report estimates that around 71% of workers of a survey made by i4CP - a HR thinktank based in United States, believe that their organizations are not prepared to face this gap. Capacity gaps can occur in various areas at the time, including the organization’s philosophies, leadership, financial management and cooperation, information technology, fundraising, and program effectiveness, among others. Nevertheless, in the 4.0 industry field different studies have pointed out that the labour demand has overcome the supply, which has generated a deficit in the new skills required by companies and organizations.

[18] CAF.: *AI Experience. Data and Artificial Intelligence in the Public Sector.* Available in: www.scioteca.caf.com. Last access: 14-10-2021.

The World Economic Forum in The Future of Jobs Report 2020 projects a 5-years perspective on the top 10 require skills: analytical thinking and innovation, active learning, creativity and initiative, emotional intelligence and problem solving, technology design and programming. It also pointed the skills whose demand was already in decline in 2020 as manual skills, memory, management of financial and material resources, and coordination and time management, among others.[19]

It estimates that by 2025, 85 million jobs may be displaced by a shift in the division of labour between humans and machines. But even more jobs - 97 million - may emerge that are more adapted to the new division of labour between humans, machines, and algorithms. In this context, greater adoption of technology will mean in-demand skills across job changes over the next five years, and skills gaps will continue to be high. For those workers who stay in their roles, the share of core skills that will change by 2025 is 40%, and 50% of all employees will need reskilling (up 4%). On the other hand, investment in digital skills training is an essential strategy to improve the employability of workers and the quality of employment.

However, one of the main drawbacks that companies face when considering implementing digital training is a cost-time benefit. Thus, it is more likely that 40% of workers will require reskilling of six months or less, but that number can vary according to the industry area. The Forum uses Coursera data, and it seems to take just one to two months to acquire skills in emerging professions across people and culture, content writing, and sales and marketing; two to three months for learners to expand their skills in product development and data and AI. While a four-month learning programme could help people move into roles in cloud and engineering. [20]

The second gap corresponds to maintain quality of work and productivity of workers through motivation. In high-performance organization there is 20% of probability for to be prepared to face this branch than in low and underperforming organizations, 6%. Although learning a new skill, reskill, and upskill set is increasingly accessible through digital technologies and e-learning, individuals will also need the time and funding to be able to pursue new opportunities, despite the current economic downturn because of the pandemic situation. Nevertheless, a large majority of employers - 2 out of 3 or approximately 66% surveyed companies, recognize the value of human capital investment and expect to get a return on investment in upskilling and reskilling within one year.

---

[19] WEF.: *The Future of Jobs Report 2020*. Available in: https://www.weforum.org/reports/the-future-of-jobs-report-2020. Last access: 14-10-2021.

[20] WEF., *These are the top 10 job skills of tomorrow - and how long it takes to learn them.* Available in: https://www.weforum.org/agenda/2020/10/top-10-work-skills-of-tomorrow-how-long-it-takes-to-learn-them/. Last access: 14-10-201.

However, the current global economic downturn turns this time horizon in risks being too long for many employers, which nearly 17% remain uncertain on having any return on the investment. According to the report, employers expect to offer reskilling and upskilling to just over 70% of their employees by 2025. Still, employee engagement into those courses is lagging, with only 42% of employees taking up employer-supported reskilling and upskilling opportunities[21]. Hereto, collaborative programs in between private and publica organizations are the key for to employees take chances and opportunities to improve their skills.

In this sense, the joint efforts made by a variety of organizations to promote high-impact and scalability solutions stand out, which is remarkable in the Latin America, thus regional and local initiatives. In a regional proposal, CAF along with the IALAB, a research center of AI associate to the Faculty of Law in the University of Buenos Aires - Argentina, launched the Multidisciplinary Artificial Intelligence Training Program aimed at professional linked to TICs, Data sciences, MD, lawyers, engineers, public servers, and entrepreneurs of all CAF's members citizens[22]. And in a local approach, we can take for example the Public Company for the Management of Innovation and Competitiveness of Guayaquil County, which was created to promote economic development and competitiveness to their citizens through mentoring in digital transformation offering digital courses and strategies for entrepreneurs and professionals that reside in the area, in a partnership with Universidad de Especialidades Espiritu Santo.[23] These programs are willing to offer solutions to narrow the digital divide as asymmetry in citizens to governments.

4.1. Digital literacy and education systems to narrowing the digital gap: Japan legal framework

The last challenge that we are going to analyze in this educational and implication to professional and workers impact, is digital literacy. There is not a defined concept of Digital literacy, it could be considered as a new emerging literacy comprising multiple dimensions and represented in new, multimodal social practices, as the sum of the other

[21] WEF.: *The Future of Jobs Report 2020*. Available in: https://www.weforum.org/reports/the-future-of-jobs-report-2020. Last access: 14-10-2021.

[22] IALAB, *Multidisciplinary Artificial Intelligence Training Program. Accelarating the AI ecosystem in Latin America.* Available in: https://ialab.com.ar/programa-de-formacion-multidisciplinario-de-inteligencia-artificial/. Last access: 14-10-2021.

[23] EPICO, *EPICO and UESS sign an agreement for programs' development and initiatives for innovation, research and links with society.* Available in: https://epico.gob.ec/epico-y-la-uees-firman-convenio-para-el-desarrollo-de-programas-e-iniciativas-de-innovacion-investigacion-y-vinculacion-con-la-sociedad/. Last access: 14-10-2021.

literacies, which include information literacy, media literacy, Internet literacy, and computer or ICT literacy, e.g., hardware and software knowledge and skills. The pandemic of COVID-19, as we mentioned by and large, have magnified the pre-existing inequalities. In this case, it was affecting access to meaningful literacy learning opportunities disproportionally to 773 million non-literate young people and adults, according to UNESCO's Global Framework of Reference on Digital Literacy Skills.

Thereby, this inequality is likely to be exacerbated by the dual impact of technology and the pandemic recession, as it has affected more individuals - lower wage workers, women, and younger workers, with lower education levels were more deeply impacted than in any other global crisis. However, there is a possible way to take some actions in order to narrow o decrease the impact on people's preparation to the Fourth Industrial Revolution by discussing and looking at what have been done properly in other regions. Thus, Japan's Plan on AI literacy must be acknowledged for this consideration.

On 28 June 2019, Law of Promotion of Informatization of School Education was promulgated for the purpose of the establishment of AI literacy education and the computerized environment at school ranging from elementary to high education level. In doing so, schools are in the process of the implementation of the STEAM education. Followingly, Japanese government published AI strategy - 戦略, in July 2019, whose plan was initiated from April 2020 in practice[24].

One of the ambitious agendas is to aim at increasing AI literacy among the 25% population of Japan, which amounts to 15 million people. 6 public universities that were chosen by the government elaborated a model of curriculum concerning AI subjects including the elements of mainly Mathematics, Data Science and AI. These universities initiated AI literacy classes as obligatory subjects for all university students regardless of their study and major. Therefore, even the ones who major in literature are required to take AI literacy classes. The model of AI literacy class is separated into three categories with optional courses.

As an introduction, the subject encompasses how AI is utilized in our society. Secondly, it deals with how to read data, how to explain data and how to treat data. Lastly, it is concerning data protection, bias and privacy issues. Moreover, there are optional courses prepared for students to deepen the subject such as learning programming. Even though their plan is trustworthy in terms of creating the base of the labour force for the digitized world, we would argue that the AI education strategy of the Japanese government has been focusing on innovation, the future and creating the

[24] AI Strategy 2019 AI for Everyone: People, Industries, Regions and Governments, Expert Group on Architecture for AI Principles to be Practiced, Artificial Intelligence Technology Strategy Council of Japan, 2019.

industry and overlooked the emerging inequality issues and the coming digital divide. It lacks the point of view of institutional support for those who are already in the labour market. This might enable a digital divide to be worse.

In Japan, the COVID-19 disclosed the digital divide in schools by region. In April 2020, only 5% of public schools established an interactive online education system. Subsequently, it increased only to less than 10%.[25] The establishment of the ICT environment in schools counted on the budget that each local government made, which resulted in inequality of the access to the education. The Japanese government decided to offer financial support for the students from low-income families with a ICT package. The process became stagnant in some local governments. The local governments only provided schools with installations, not substantive support. Therefore, in some schools where there are not any people who are not familiar with ICT, the implementations were not done efficiently.

As a result, the inequality was recognized in the access to the education between the low income and the high-income family, depending on whether they have a sufficient internet connection and related devices and how much knowledge they possess regarding ICT. The digital divide in schools proceeded at a regional level and an individual level.

V. CONCLUSION - DIGITAL DIVIDE AND THE DIGITAL FUTURE IN THE PACIFIC REGION

In the times of the Fourth Industrial Revolution everything seems to occur at the same space-time, yet when we analyze different regions, it appears to be creating or exploring other realities. The challenge is not only physical or infrastructural but cultural and mental issues too. The Japanese and Asia-Pacific countries strategy to diminish a digital divide mainly dealt with the enhancement of accessibility through infrastructure. Meanwhile in Latin America other inequality factors undermine the pursuit of innovation for the market and industry and life's quality to individuals, in addition to lack of resources, investment on talent and brain drain.

The recognition of digital gap or divide as an issue, is a clear demonstration of the branch in terms of development and social-economic evolution. For instance, digital divide was recognized in Japan in the earliest stage of automatization, in the White Paper 2000 Report as a social issue. In Ecuador, it was identified in 2016, when the OECD report was launched, even though in 2008 it was declared in the Ecuadorian Constitution

[25] Teachers and students are in the virtual class face to face through a camera. Mandatory education is from 6 to 15 years old students.

the right to access to TICs and Internet. In doing so, digital divide has also transformed from a traditional sense, e.g., not having Internet access, to a new and complex aspects, e.g., upskilling and reskilling in professionals. And finally, inequality caused by knowledge regarding an effective usage of new technologies; to what extent people make full use of new technologies. It is regarding the literacy of new technologies the key to diminish digital divide, as it is imperative to shift from an Information Society to a Smart-Inform society, where professionals, workers, organizations, and governments cooperate on narrowing inequality factors.

VI. REFERENCES AND BIBLIOGRAPHY

ARNTZ, M., GREGORY, T. y ZIERAHN, U.: "The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis", *OECD Social, Employment and Migration Working Papers*, nº 189, OECD Publishing, Paris, 2016.

CAF: *AI Experience. Data and Artificial Intelligence in the Public Sector*. Available in: www.scioteca.caf.com. Last access: 14-10-2021.

China Innovation Funding, *State Council's Plan for the Development of New Generation Artificial Intelligence.* Available in: https://chinainnovationfunding.eu/dt_testimonials/state-councils-plan-for-the-development-of-new-generation-artificial-intelligence/. Last access: 13-09-2021.

GSMA. *Over Half World's Population Now Using Mobile Internet*. Available in: https://www.gsma.com/newsroom/press-release/over-half-worlds-population-now-using-mobile-internet/. Last access: 12-09-2021.

GSMA, *The mobile Economy in Latin America 2020.* Available in: https://www.gsma.com/mobileeconomy/latam/. Last access: 14-09-2021.

CAF, *Digital Transformation for 21st-Century Latin America*. Available in: https://www.caf.com/en/knowledge/views/2020/02/digital-transformation-for-21st-century-latin-america/. Last access: 14-09-2021.

EPICO, *EPICO and UESS sign an agreement for programs' development and initiatives for innovation, research and links with society.* Available in: https://epico.gob.ec/epico-y-la-uees-firman-convenio-para-el-desarrollo-de-programas-e-iniciativas-de-innovacion-investigacion-y-vinculacion-con-la-sociedad/. Last access: 14-10-2021.

IALAB, *Multidisciplinary Artificial Intelligence Training Program. Accelarating the AI ecosystem in Latin America.* Available in: https://ialab.com.ar/programa-de-formacion-multidisciplinario-de-inteligencia-artificial/. Last access: 14-10-2021.

JARAMILLO, C. F.: *Closing the digital gap to end poverty in Latin America and the Caribbean.* Available in: https://blogs.worldbank.org/latinamerica/closing-digital-gap-end-poverty-latin-america-and-caribbean. Last access: 13-09-2021.

LAW, N. WOO, D. DE LA TORRE, J., and WONG G.: *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2*, University of Hong Kong and UNESCO, Quebec, 2018, p. 6.

MIC-ICT.: *White Paper 2020 - Information and Communication in Japan 2020 summary*, Ministry of Internal Affairs and Communications, Tokyo, 2020, p. 3.

NITTO, H., TANIYAMA, D. and INAGAKI, H.: "Social Acceptance and Impact of Robots and Artificial Intelligence - Findings of Survey in Japan, the U.S. and Germany"*, NRI Papers*, nº 211, 2017, p. 2.

OECD.: *Latin American Economic Outlook 2020.* Available in: https://www.oecd.org/dev/latin-american-economic-outlook-20725140.htm. Last access: 13-09-2021.

OCDE. "Social impact of COVID-19 in Ecuador: challenge and responses", *Making Development Happen*, Vol. 4, 2020. p. 8.

PETERSON, D.: "Designing Alternatives to China's Repressive Surveillance State", *CSET Policy Brief,* Georgetown's Walsh School of Foreign Service, Washington D.C, 2020, p. 10.

SOLAR CAYÓN, J. *La inteligencia artificial jurídica. El impacto de la innovación tecnológica en la práctica del Derecho y el mercado de servicios jurídicos*. 1ª ed., Aranzadi, 2019, p. RB-1.3.

UNESCO, *Literacy.* Available in: http://uis.unesco.org/en/topic/literacy. Last access: 14-10-2021

WEF, *The Future of Jobs Report 2020*, World Economic Forum, Geneva, 2020. Online version available in: https://www.weforum.org/reports/the-future-of-jobs-report-2020. Last access: 14-10-2021.

WEF, *These are the top 10 job skills of tomorrow - and how long it takes to learn them,* World Economic Forum, Geneva, 2020. Online version available in: https://www.weforum.org/agenda/2020/10/top-10-work-skills-of-tomorrow-how-long-it-takes-to-learn-them/. Last access: 14-10-201.

Women in Tech: *Why we exist*. Available in: https://women-in-tech.org/context/. Last access: 14-09-2021.

World Bank, *World Development Report 2016: Digital Dividends*, World Bank Publications, Washington D.C, 2016, p. 2.

REGULATION OF THE DIGITAL ECONOMY FOR PROTECTION AGAINST LARGE PLATFORMS

Por

ANDRÉS BOIX PALOP / ALBA SORIANO ARNANZ
Lecturers in Administrative Law
University of Valencia

Revistas@iustel.com

Revista General de Derecho de los Sectores Regulados 8 (2021)

This monographic issue of the Revista General de Derecho de los Sectores Regulados, published by Iustel, which is the eighth number of this journal, thus reflecting its full consolidation, is a great satisfaction for us. Firstly, because of the possibility of having compiled, selected and reviewed these works for publication in a journal such as this one, which is already well established and with a proven track record of quality, and which is leading academic reflection on the legal regime of sectors which are becoming increasingly important and in need of publications with the rigour and usefulness of this one. Secondly, because we believe that the final result of the compilation we have achieved is of enormous interest, shedding legal light on some of the most topical issues regarding the regulatory challenges posed by the growing emergence of digital platforms in more and more sectors of economic activity, in a position as intermediaries which, thanks to the technology they use and the efficiency gains they have generated, gives them enormous market power. Finally, because these works constitute part of the results of initiatives for the internationalisation of legal research that we have been trying to promote from various research groups at the University of Valencia, which, in our modest opinion, are beginning to bear excellent results. The papers presented in this issue have been selected from among the proposals that were finally accepted for presentation at the Summer School of the Jean Monnet European Network on Sharing Economy and Inequalities Across Europe (SHINE) held in July 2021 at the Universitat de València on the study of issues such as the digital economy, technological innovation and its effects on inequalities (Digital Economy, Technology and Inequalities).

We have entitled the monograph "The regulation of the digital economy for protection against large platforms" because we believe that most of the reflections we have selected

are threaded around this idea, as well as the added value that, in our opinion, they can provide from the study of these conflicts.

The monograph opens with studies on the regulation of these markets in order to contain the risks that the growing control of the large platforms may pose to them, beginning with the work of one of us (Andrés Boix Palop, Universitat de València: Digital Platform Competition Regulatory Challenges") on the challenges that the peculiar position that digital platforms have achieved and some of the characteristics of the functioning of the digital economy pose when it comes to applying in a useful way the traditional competition guidelines that had been established by our competition authorities in recent years based on their analysis of anti-competitive dynamics in other types of markets. The conclusion is that some of these guidelines no longer serve to contain the effective competition problems, and also social problems, that can be generated by the new positions of dominance in the digital economy and that, consequently, some of these criteria need to be adapted.

Next, José Vida Fernández (Universidad Carlos III de Madrid) offers us "Una aproximación al régimen jurídico de los servicios digitales: estructura y sistemática del marco jurídico de los servicios prestados en línea", where he tries to expose in a synthetic, clear and complete way the structure of the legal framework referred to European (and Spanish) digital services, structuring it in an orderly and systematic way, where the legislator (or the concurrence of legislators) have been rather disorderly, in order to help us to determine the legal regime applicable to each of these services within the digital environment.

In a clearly complementary line, Carmen Rodilla Martí (Universitat de València) explains in her paper "Digital platform markets: between competition law and regulation" how the integration processes of these platforms and their growing market power require a combined use of Competition Law tools, but duly adapted and sharpened, together with the establishment of regulatory guidelines specifically designed to control these new hegemonic operators, with the added value of proposing some (and very interesting) specific solutions.

A third work, also more focused on the regulation of the activity of these platforms and the control of some of the pernicious effects that may arise for certain collective and individual interests, through the establishment of specific legal rules that seek to maximise the benefits of their activity and contain some of the possible abuses that may occur in the digital economy, is the study presented by Michael Fehling and Nico Schröter (Bucerius Law School, Hamburg). Their work, "Social aspects (working conditions and consumer protection) of the digital economy in the mobility sector: a challenge for regulation", is focused on a specific sector, transport markets, of a huge economic importance and in which digital intermediation has achieved a significant degree of maturity, thus bringing it

to the forefront of conflict. In addition to a precise dissection of the regulatory situation, the analysis includes a very interesting call for solutions through more and more demanding self-regulation.

More transversal is the work of another of us (Alba Soriano Arnanz, Universitat de València: "La propuesta de Reglamento de Inteligencia Artificial de la UE y los sistemas de alto riesgo"), which focuses on analysing how, at the European level, an increasingly demanding regulatory model is being constructed for the uses of artificial intelligence and the various algorithmic tools that these large platforms use, in an increasingly refined and precise manner, for their intermediation and processing of information on users, their preferences and the functioning of the markets in which they operate. Focusing on the analysis of the recently presented proposal for the EU Regulation on Artificial Intelligence, the study dissects the specific high-risk problems, the mechanisms envisaged to control them and assesses their viability and sufficiency.

In addition to these first papers, which focus more on the structure of these markets, their regulation and the dynamics of competition, a second block of papers analyses in detail and rigour some of the problems more closely linked to the dynamics of private law, relations between platforms and between platforms and consumers. These works begin with the article by Mireia Artigot Golobardes (Universitat Pompeu Fabra, Barcelona) on automated contracting, which raises the limits that traditional contract law and the current data protection legal framework present when dealing with algorithmic contracting and, in particular, when protecting weaker parties (“Las inherentes limitaciones del modelo autodeterminista de protección de datos en Europa”).

Along the same lines, but starting from the definition of the problem and seeking solutions, Sébastien Fassiaux (Universitat Pompeu Fabra, Barcelona) proposes possible solutions that involve, precisely, combating some of the problems that may be a consequence of the transformations brought about by technology with technological solutions and, specifically, establishing as legally necessary in a series of cases default systems, directly derived from the design of the platform and its programming, which determine greater privacy.

Completing these reflections, María L. Mena (King's College, London) presents an interesting reflection on some of the consequences of the so-called "smart contracts" and the use of technologies such as blockchain and distributed registration systems in general, highlighting the challenges they pose in the contract formation phase in her paper "Towards the dehumanization of the contract formation phase. Algorithmic contracting and smart contracts".

Edoardo Vinchesi (Università Ca'Foscari, Venice) closes this block with his paper "The social network profile shutdown in the digital identity perspective", which analyses recent

judicial decisions in Italy. The paper analyses recent court decisions which, in Italy, have recognised the cancellation of digital profiles without justification as grounds for the recognition of compensation for non-pecuniary damages (in accordance with article 2059 of the Italian Civil Code), as it is understood that these decisions, if they have not been correctly and thoroughly agreed by the parties, may represent a clear example of abuse on the part of the platforms towards their clients and consumers.

Finally, Akihisa Hirano and Victoria Granda (Universitat de València) close the monograph with a case study on the effects of the digital economy as a factor of inequality, analysing the first data on the consequences in two very different economies in the Pacific region, Japan and Peru. Their paper "Digital divide as an inequality factor. A study for the digital future in the Pacific Region" provides very interesting data in this respect and a different perspective on the adaptation of different societies and development models to the effects and transformations caused by the digital economy, which must lead to different regulatory strategies to combat inequality.

In our opinion, all the papers presented provide a very interesting immersion into some of the problems, whether related to the necessary regulation of these markets from a public-legal perspective or in terms of competition law and the prevention of abuses of dominant positions, whether they are defined on the basis of the particularities of the new digital intermediation markets, whether they are related to the conflicts generated by some of their instruments (such as algorithms and artificial intelligence) in their different modalities, or whether they refer to questions of contracting with consumers and the protection of the weaker parties in the legal relationships that arise in these markets. We hope that it will be interesting and, above all, useful reading for the readers of the Journal and, more generally, for all those interested in the study of these issues.

València, 2 November 2021

Andrés Boix Palop and Alba Soriano Arnanz
Lecturers in Administrative Law
University of Valencia

The publication of this monograph has been made possible in part thanks to the support of the Erasmus Programme of the European Union, channelled through the Jean Monnet Network "Sharing Economy and Inequalities across Europe" (611585-EPP-1-2019-1-ES-EPPJMO-NETWORK).

With the support of the Erasmus+ Programme of the European Union