Universidade do Minho
Escola de Direito

Thiago Vinícius Vieira

Convergence between Competition and Data Protection Legal Setting: Protecting Startups by Studying a Fair Competition Mechanism

julho de 2020

Convergence between Competition and Data Protection Legal Setting: Protecting Startups by Studying a Fair Competition Mechanism
Thiago Vinícius Vieira
UMinho | 2020

Universidade do Minho
Escola de Direito

Thiago Vinícius Vieira

Convergence between Competition and Data Protection Legal Setting: Protecting Startups by Studying a Fair Competition Mechanism

Dissertação de Mestrado
Mestrado em Direito dos Negócios Europeu e Transnacional

Trabalho efetuado sob a orientação da
Professora Doutora Joana Rita Sousa Covelo Abreu

julho de 2020

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho

Atribuição-NãoComercial-SemDerivações
CC BY-NC-ND

https://creativecommons.org/licenses/by-nc-nd/4.0/

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

Convergence between Competition and Data Protection Legal Setting:

Protecting Startups by Studying a Fair Competition Mechanism

ABSTRACT

The theme of this dissertation refers to the convergence between competition and the legal environment of data protection: protecting startups through the study of a fair competition mechanism. The development of science is based on obtaining results that allow validating hypotheses about a given event or fact, present or not in society. The specific objectives seek to present and highlight the role of data in the economy and on the internet, as well as to highlight the right of jurisdiction according to the European Union, in addition to addressing data protection and competition law in the European Union, and finally, present the abuse of dominant position of the technology titans in the current context. Finally, the present work leaves the topic open, proposing that a new research be carried out in the future, in order to contextualize the themes addressed here. Along with this new research, it is suggested to carry out a case study, for which a comparative study between European legislation on data protection law with Brazilian law is proposed.

Keywords: Competition, Data protection, European Union, Startups.

Convergência entre concorrência e as leis de proteção de dados:

Protegendo as startups através de um estudo do mecanismo de concorrência leal

RESUMO

O tema deste trabalho refere-se à convergência entre a concorrência e o ambiente jurídico da proteção de dados: protegendo as startups através do estudo de um mecanismo de concorrência leal. O desenvolvimento da ciência baseia-se na obtenção de resultados que permitem validar hipóteses sobre um dado evento ou fato, presente ou não na sociedade. Os objetivos específicos buscam apresentar e destacar o papel dos dados na economia e na internet, bem como evidenciar e salientar o direito de competência segundo a União Europeia, além de abordar a proteção de dados e direito da concorrência na União Europeia, e por fim, apresentar o abuso de domínio dos titãs da tecnologia no contexto atual. Por fim, o presente trabalho deixa o tema em aberto, propondo que no futuro se realize uma nova pesquisa, com a finalidade de contextualizar os temas aqui abordados. Juntamente com esta nova pesquisa, sugere-se a realização de um estudo de caso, para o qual propõe-se um estudo comparativo entre as legislações europeias sobre o direito de proteção de dados com a legislação brasileira.

Palavras-chave: Concorrência, Proteção de dados, Startups, União Europeia.

SUMMARY

LIST OF FIGURES

LIST OF ABBREVIATIONS

% - percentage

€ - euro

ACT - California Consumer Privacy

AI - Artificial Intelligence

API - Application Programming Interfaces

Art. - Article

B2B - data sharing

B2G - data sharing business-to-government

CCPA - California Consumer Privacy Act

CDT - Center for Democracy & Technology

CJEU - Court of Justice of the European Union

CNIL - French Information and Freedoms Commission

CNPD - Portuguese Data Protection Authority

CPI - Competition Policy International

CRM - Customer Relationship Management

D-NY - New York District

DPA - Data Protection Authorities

DPO - Data Protection Officer

e.g. - Exempli gratia

EC - Council Regulation

EC - European Commission

ECJ - Justice of the European Union

EDPB - European Data Protection Board

EDPB - European Data Protection Council

EEA - European Economic Area

EPIC - Electronic Privacy Information Center

ESM - European Startup Monitor

EU - European Union

EUR - Euro

EU-US - European Union/United States of America

FTC - Federal Trade Commission

G2B - data sharing government to company

GDPR - General Data Protection Regulation

GPS - Global Positioning System

GRPD - EU General Data Protection Regulation

ICA - Italian Competition Authority

ICC - Court of First Instance

ICO - Initial Coin Offering

Inc. - Incorporated

INPLP - International Network of Privacy Law Professionals

ITA - International Trade Administration

LOPD - Organic Law on the Protection of Personal Data

M&A - Mergers and Aquisitions

ML - Machine Learning

MVP - Minimum Viable Product

N.V. - Naamloze vennootschap

NGOs - Non-governmental organization

No - Number

OECD - Organisation for Economic Co-operation and Development

OEMs - Original Equipment Manufacturer

ONS - Office for National Statistics

PCs - Personal Computers

PETs - Privacy Enhancing Technologies

SA - Supervisory Authority

SaaS - Software as a Service

SEC2SV - Startup Europe Comes to Silicon Valley

SEP - Startup Europe Partneship

SIEC - Significant Impediment to Effective Competition

SMEs - Small and Mid-size Enterprises

TFEU - Treaty on the Functioning of the European Union

TfL - Transport for London

TICs - Communication technologies

U.S. - United States

UK - United kingdom

USA - United States of America

UWG - Unfair Competition Act

UX – User Experience

I. INTRODUCTION

In economics, the definition of competition refers to when several companies compete in a market to offer their products or services to a group of consumers who act independently and integrate demand.[1] Thus, different economic agents who participate in a market apply better strategies so that they can obtain a limited good and be able to minimize their costs, maximize their profits and remain active and innovative compared to other agents. It also refers to the rivalry between companies that participate in a given market, developing their best strategies with the objective of increasing profits, minimizing costs and thus being able to compete in the best possible conditions with other companies in the sector.[2]

The concept of competition is a logical derivative of free markets, where the decision-making power of the stock market rests with consumers and their evaluations of the products that interest them. One of the essential aspects of economic competition lies in people's freedom to produce and market the products they want and the way they want it. This ends up generating a number of competitors based on buyer preferences. Undoubtedly, what ends up influencing a competitive market are prices. Companies that put the lowest value on their items and are willing to get the lowest percentage of sales profit are usually the most successful. However, they sometimes face a certain commercial risk that may jeopardize the future of the company.[3]

Therefore, economic agents strive to improve the use of resources to produce goods and services, improving and innovating in the quality and variety of these. It results in improvements in competitiveness and more benefits for the consumer, all to achieve greater economic growth and social well-being.[4]

It is essential to establish competitive advantages to differentiate the company's products or services, when positioning itself as a leader in a commercial market. This differentiation can ultimately be real or perceived by the customer or suppliers. By taking into account the real differentiation, it is able to create of products that are not yet available on the market. However, perceived differentiation requires a little more work on the part of the company, as it requires advertising tools that show the product with differences in relation to the competition[5].

---

[1] Aumann, R. & Hart, S. (eds.) (1994). *Handbook of Game Theory with Economic Applications* (*2*). ch. 30: "Voting Procedures" and ch. 31.
[2] Craig, P. & Burca, G. (2008) EU LAW, Text, Cases and Materials (Sixth Edition, p. 1074). Oxford University Press.
[3] Kuhnert, J. & Leps, O. (2017). *Wohnungsgemeinnützigkeit Neue* (pp. 213-258). Springer Wiesbaden Fachmedien.
[4] Kusters, M. (2013-2014). *Competition Law*: The Concept of Abuse in New Technologies: time for Adaptations? Belgium: KU Leuven, p. 12.
[5] Lag, 2013.

Markets are generally subject to private or state restrictions on competition - for example, in the presence of a cartel or monopoly. Private property rights, freedom of trade, freedom of establishment, freedom of contract, functional judiciary, functional pricing system, functional monetary system, market transparency and market opening are, therefore often considered prerequisites for the functioning of competition.[6]

A company's competition can be understood in different ways, but ultimately it is about overcoming competition in the industry by using commercial and business tools to acquire a dominant position for business in that market.[7] It should not be forgotten that any competitive company must offer quality, reliability, speed and flexibility, in addition to profitability. Accordingly, these factors perform different functions, depending on the characteristics of the company, such as size and sector, degree of competition, among others. Each company and business must establish for its sector the necessary capabilities to develop its competitiveness in the market.[8]

When it comes to microeconomics, it usually refers to the study of competitiveness at the company level. Companies are considered competitive if they can generate long-term profits in the domestic and/or international markets and at the same time compete with other companies in the same market sector. Today's markets have a lot of competitive pressure; therefore, companies need to measure themselves in relation to various sizes, models, prices, level of awareness, location etc. These are common means of measuring competitiveness. A company that cannot assert itself in the market and does not have a specific position is therefore putting its existence at risk. Thus, competition in a market-based economy decides on the existence or disappearance of a company.[9]

Trade, especially retail, has numerous competitive characteristics. One of these is the typical double involvement of commercial companies in interformal and intra-formal competition. This involvement means that a competitor can have a greater influence on general competitiveness than competing companies of the same type of enterprise. Then, the different locations may have very different degrees of competitiveness for individual companies in a retail group, for the individual subsidiaries of a subsidiary, and for individual member companies of a group of retailers.[10]

A modern development of the so-called dynamic competition model can be found in Wolfgang Kerber's theory of evolutionary competition, which transfers the struggle for survival from evolution to competitive relationship. It combines the elements of variation and selection with the assumption of

[6] Wich, R. (2018). *Competition Law.* Oxford: Oxford University Press, p. 829.
[7] Aumann & Hart, op. cit., 1994, p. 9.
[8] Lag, 2013.
[9] Craig & Burca, op. cit., 2003, p. 6.
[10] Kusters, op. cit., 2013-2014, p. 12.

incomplete knowledge of the evolution thinking model, as follows: providers test what the customer likes in each product, they choose between providers (selection) and "reward" by buying the supplier with the best deal. The competing supplier that is left behind can only change its offer (variation) by lowering the price or improving the quality or in other ways trying to get the customer's favor.[11]

This "knowledge creation competition process" increases suppliers' knowledge of customer preferences and customer needs (at best) are better met. This theory has two advantages: as one of the few theories of competition, it not only looks at the supplier side, but also integrates the process of competition to the supplier-customer relationship. This theory can also be applied in practical competition policies, notably in the control of mergers of the EU Commission[12]

The goal of favoring competition has been in economic policy for years. In March 2000, the Lisbon European Council put it on the agenda when it called for the Lisbon Strategy to make the European Union the most competitive and dynamic knowledge economy in the world. Each Member State was asked to implement targeted policies. In Luxembourg, for example, the Tripartite decided in early 2003 to set up a Competitiveness Observatory to monitor the tasks involved.[13]

The concept of "competition" obviously stems from the administration of companies, where it clearly refers to the internal and external relations of an enterprise. In particular, it means in this area the ability of a company to increase its market share in a competitor's environment. This conceptual meaning cannot be applied to economies and can even lead to a misimage of international economic relations as an unquestionable slogan and can result in great damage when implemented in politics. The Luxembourg government, for example, used the following definition: The competitiveness (competition) of an economy is its ability to generate permanent income, as well as high levels of employment and social cohesion, in international competition.[14]

In the crisis of the global economy, the competitiveness of the whole EU is once again in the spotlight. As euro zone countries represent a single currency area, no member country has a chance to follow its own monetary and monetary policy. Failure to counteract this loss of sovereignty and loss of governance can result in competitive disadvantages for all EU members.[15]

The term digital revolution describes the uprising triggered by digital technology and computers, which has caused a change in almost every area of life in many countries since the end of the 20th century and leads to a digital world – similar to the industrial revolution that drove industrial society 200

[11] Whish, R., & Bailey, D. (2012). Competition Law (7th Edition). Oxford: Oxford University Press.
[12] Kuhnert & Leps, op. cit., 2017, p. 17.
[13] Lag, 2013.
[14] Kuhnert & Leps, op. cit., 2017, p. 22.
[15] Essays, U. K. (2018). *Competition between companies with the same product marketing trial*. Available at: https://www.ukessays.com/essays/marketing/competition-between-companies-with-the-same-product-marketing-essay.php?vref=1

years earlier. That is why we are talking about a third industrial revolution or, in technical terms, a microelectronic revolution.[16]

The changes associated with the digital revolution in the world of business and work, in public and private life, are taking place at an accelerated pace, whenever there are material requirements for applications and uses of advanced scanning. New media are increasingly influencing communication behavior, socialization processes, language culture, the way it consumes and what is consumed. Areas of application and development potential of artificial intelligence are among the trends and open future issues of the digital revolution. Following these advances, it is extremely important to adapt the other sectors, such as economic, market, political, legislative, among others, in view of the advances achieved.[17]

Globalization and digitization are changing our economy and society. The determining factors of this development are often online platforms and global digital companies with new data-driven business models. It cannot be denied that the market has received major impacts in the digital age, the way products are consumed have changed and even the products that are consumed not only change but rapidly evolve. Nowadays, everyone is connected to the internet in some way and through various websites and applications, where the most diverse personal data of users are hosted.[18]

It is worth noting that just as new technologies emerge, innovative companies are been created everywhere, raising concern about establishment of rules for market competition. Taking account that access to data in the future is has great importance and value, the emergence of new data monopolies should be avoided. Therefore, there must be opportunities in competition law to sanction the abusive refusal of data as a breach of competition and to be able to request access or sharing of data.[19]

Considering the worries above, on 16 January 2019 the European Commission published a report[20] prepared by a panel of three academics on the subject of competition policy in the digital age. The aim of this report is to analyze possible adaptations of competition law to the digital age in order to ensure innovation for the benefit of consumers. Thus, within this context, the present work will seek to answer the following questions:

a) To what extent is it possible to study a fair competition mechanism protecting startups through the convergence between competition and a legal data protection environment?

[16] Wich, op. cit., 2018, p. 10.
[17] Kusters, op. cit., 2013-2014, p. 5.
[18] Wich, op. cit., 2018, p. 77.
[19] Essays, op. cit., 2018, p. 56
[20] Reference needed. European Commission published a report on 16 January 2019.

b) What are the pillars of privacy in mergers (as a competition parameter)? What is the real imposition of large fines on small businesses (startups) - disproportionate?
c) What are Startups/companies that do not obey/do not comply with data privacy rules that compete with others that do? Why the former do not just respect privacy rules?
d) Why is the privacy shield no longer in effect? Why cannot some newborn startups just bear the cost of litigation?
e) Finally, because privacy legislation can increase barriers to entry through increased compliance and legal costs. Are larger established companies often in a better position to absorb these costs at the expense of smaller competitors and potential participants?

Thus, the present work will seek, through its general objective, to present the convergence between competition and the legal data protection environment, protecting startups and studying a fair competition mechanism. The specific objectives will seek to present and highlight the role of data in the economy and on the internet, as well as the right of jurisdiction according to the European Union, in addition to addressing data protection and competition law in the European Union, and finally, present the abuse of dominance of the technology titans in the current context.

This research is justified as a means of contributing to the academic environment, contextualizing and enriching the theme regarding the convergence between competition and the legal data protection environment: protecting startups by studying a fair competition mechanism. This research is also justified, as a means of simplifying this theme in its social environment, seeking to present a concise and easily assimilated material by lay readers who seek a deeper knowledge on the subject.

The development of science is based on the achievement of results that allows to validate hypotheses about a given event or fact, present in our lives, or not. According to Gil[21], research is of fundamental importance for the evolution of knowledge in a given field of study, that is, through research one can broaden the horizons of knowledge on a given theme.

The bibliographic research was carried out the preparation of this review, where the material was read; identification of the information and the data contained in the printed material; establish relationships of the information and data obtained with the proposed problem; and analysis of the consistency of the information and data presented by the authors. Bibliographic research seeks to

[21] Gil, 2002.

explain and discuss a theme based on theoretical references published in books, journals, journals and others. It also seeks to know and analyze scientific contents on a given theme.

Data collection was developed following the following premises: Exploratory reading of all selected material, whether objective reading or a quick reading, in order to verify whether the work, document and complementary material is of interest to this research.

In addition to this reading model, the selective reading model had been adopted, which consists of a reading with a greater depth, seeking consistent material for the work. Finally, the information extracted from the sources was recorded, being specified in the work, with name and year of publication.

The analysis was guided by the general and specific objective of the study, evidencing in three stages: Pre-analysis, Exploration of the material and Treatment of the obtained data and interpretation, for a better understanding. An analytical reading of all material was also performed, with the purpose of ordering it and summing up the researched and elaborated information. In this process, the information that would enable the response of the research problem to be obtained was taken into account, through the general and specific objectives.

II. THE ROLE OF DATA IN THE ECONOMY AND INTERNET

II.1 The Concept of Startups

The Internet has revolutionized everything, the way society communicates, its way of organizing and behaving in the day to day, what is consumed and even the way to start a business. Previously, the idea of starting a business or company seemed only possible for these great characters with significant capital, but the invention of new technologies allowed anyone to realize their dreams through startups.[22]

However, before talking about startups properly, the term must be interpreted. A startup or start-up is a project, not yet necessarily a company, started by an entrepreneur or a group of entrepreneurs to seek to effectively develop and validate an innovative product, not necessarily an invention, with a scalable business model.[23]

Author Kaiser and Müller[24] defines startup as a newly created company that markets products and/or services through the intensive use of information and communication technologies (TICs), with a scalable business model that allows it to grow rapidly and sustain itself over time. In Salamzadeh's[25] view, although the word Startup is a business-linked concept in the digital age, it is also a measure of time. That is, the startup is a great company in its early stage; Unlike a Small and Mid-Size Enterprise (SME), Startup is based on a business that can be scaled faster and easier, using digital technologies.[26]

The authors Davila, Foster & Gupta[27], define startup as a human organization with great capacity for change, which develops highly innovative products or services, highly desired or demanded by the market, where its design and marketing are totally customer oriented. This structure generally operates at minimal costs, but generates profits that grow exponentially, maintains continuous and open communication with customers, and is focused on mass sales.

Each startup is supported by an idea that seeks to simplify complicated processes and tasks, with the goal of the market having a simplified and easy user experience. Generally, they are companies that want to innovate, develop technologies and design web processes. Mostly, they are venture capital

---

[22] Blank, S.; Dorf, B. (2012). *Startup*: Entrepreneur's Manual. São Paulo: Alta Books.

[23] Robehmed, N. (Dec 16, 2013). *What is a startup*? Available at: https://www.forbes.com/sites/natalierobehmed/2013/12/16/what-is-a-startup/#e0b766340440

[24] Kaiser, U. S. & Müller, B. (2013). *Team heterogeneity in startups and its development over time* (Discussion Paper, 13-058). Available at: http://zinc.zew.de/pub/zew-docs/dp/dp13058.pdf

[25] Salamzadeh, A. (June 14, 2015). Innovation Accelerators: Emergence of Startup Companies in Iran (pp. 6-9). In: *60th Annual ICSB World Conference*. Dubai: UAE. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2618170

[26] Colombo, M.G.; Piva, E. (January 22, 2008). Strengths and weaknesses of academic startups: a conceptual model. In*: IEEE Transactions on Engineering Management*. *Strong and weak academic startups: a conceptual model*, DOI: 10.1109/TEM.2007.912807, *55*(1), pp. 37-49. Available at: https://ieeexplore.ieee.org/document/4439878

[27] Davila, A., Foster, G. & Gupta, M. (2003). Venture capital financing and the growth of startup firms. *Journal of Business Venturing*, *18*(6), pp. 689-708.

firms. Not everyone should or has the opportunity to work in large companies, and that is the degree of importance that a startup has.[28]

As the name implies, the term only applies when the project is at startup. Once scaled, it will no longer be called Startup. Major tech giants such as Facebook, Google, Airbnb or Uber started out as Startups; however, at that time, they could no longer be considered in this area. Scalability, which has to do with the company's potential growth, is the second fundamental aspect of a startup.[29]

In addition to being characterized as profitable companies, Startups are known for offering creative and different solutions to these problems. It is not about looking for strange or unimaginable solutions, but about thinking about simple strategies, but that no one has put into practice before (or that no one has done it well enough).[30]

Today, the concepts of startups and Small and Mid-size Enterprises (SMEs) are often confused. However, there are differences. According to the European Union (EU) in its Regulation No 651/2014, the European Commission determines as micro-enterprises companies with less than 10 employees and with a turnover or Balance Sheet equal to or less than 2 million euros. To be a small business it must have fewer than 50 full employees and a turnover or balance sheet of EUR 10 million or less. The medium-sized company has fewer than 250 employees and its revenues are equal to or less than 50 million euros.[31]

According to this regulation, startups can be included in any of these categories if they reach the values indicated in the first three years. A scalable and repeatable business model, with high growth potential and existence of less than three years, are its differentiating notes. Generally, micro and small companies seek to increase their turnover with a business model already defined and tested in the market, regardless of their years of life or existence.[32]

An important moment of a startup is when the business model is considered disruptive and innovative, with rapid growth, and when turnover grows at a rate of 20% per year for more than three consecutive years (thanks to the fact that they have managed to validate their product in the market), or reach over a million dollars in funding. Then, emerges the option of scaling up. In the end, every startup can become a "unicorn" in the entrepreneurial ecosystem.[33, 34]

---

[28] Edison, H., Smørsgård, N. M., Xiaofeng, W. & Abrahamsson, P. (2018). "Lean internal startups forsoftware product innovation in large companies: enablers and inhibitors". *Journal of Systems and Software*, *135*, pp. 69-87.

[29] Chang, S. J. (2004). "Venture capital financing, strategic alliances and initial public offerings of Internet startups". *Journal of*, *19*(5), pp. 721-741.

[30] Blank & Dorf, op. cit., 2012, pp 10-12.

[31] Frederiksen, D. L. & Brem, A. (2017). How do entrepreneurs think they create value? A scientific reflection of Eric Ries's startup approach. *International Entrepreneurship and Management Journal*, *13*(8), Issue 1, pp. 169-189.

[32] Picken, J. C. (2017). "From startup to scalable enterprise: laying the foundation". *Business Horizons*, *60*(5), pp. 587-595.

[33] Unicorn is a startup that has market price valuation worth more than 1 billion dollars. The term was coined in 2013 by Aileen Lee. Some examples of unicorn companies include Loggi, Nubank, 99, Movile, TFG, EBANX and Paypal.

[34] Robehmed, op. cit., 2013, pp. 18-20.

II.1.1 EU Policies on Startups

Currently, the European Union aims to promote the growth and consolidation of technology startups and innovative SMEs on an international scale, since it is very difficult to reach this level domestically.[35]

Thus, in the European Union, the contribution is currently made under the project "Startup Europe", which seeks to connect all the actors of today's so-called "European entrepreneurship ecosystem". The Project in 2017 represented an EU fund of €10 million to boost technology companies in Europe and led the growth of more than 700 startup projects. Of these, ten European projects connect 16 cities to more than 100 internationalization activities, generating 3,500 jobs and attracting 200 million euros in investments.[36]

Startup Europe is a European Commission initiative designed to connect startups, investors, accelerators, entrepreneurs, corporate networks, universities and media across a variety of networks. In addition, it aims to connect ecosystems of local startups across Europe and improve its ability to invest in other markets such as Silicon Valley, India and Israel.[37]

It thus promotes the creation of a true entrepreneurial ecosystem throughout the European Union. In Europe, technological entrepreneurship is very local. Then, there is still no transnational ecosystem that startups can take advantage of growing, getting the resources they need in same pattern as companies of a certain size have been doing with the internal market for several decades. This community initiative is one of the tools the committee used to lay the foundations for the digital single market.[38]

It is paramount to highlight the pan-European view of different platforms. On the one hand, Startup Europe Partnership (SEP), promoted by startup Europe and the European Commission, is the open and integrated platform for pan-European innovation that helps the best climbs in the European Union to grow. In this platform, the best escalations serve the best companies and investors. It also

[35] Grilo & Irigoyen, 2006.

[36] European Commission. (Feb. 19, 2020). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions*: Shaping Europe's digital future. Brussels. Available at: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

[37] Herrmann, B. L., Gauthier, J. F. & Holtschke, D. et al. (2015) "The Startup Ecosystem Report Series 2015". Available at: http://startup-ecosystem.compass.co/ser2015/

[38] Barreneche García, A. (2013). "Analyzing the Determinants of Entrepreneurship in European Cities". *Small Business Economics*, DOI: 10.1007/s11187-012-9462-8 *42*(1), pp. 77-98.

connects the "European ecosystems" to Silicon Valley (Mission sEc2sV) and Israel (Mission sEc2 1L).[39] [40]

On the other hand, there is the Startup and Scaleup Initiative, based on a communication from the European Commission launched in 2016, whose two main objectives are: removing barriers to expansion in the single market with ecosystem-building projects and developing opportunities for networks, improving the startup ecosystem, connecting local clusters, people and ecosystems across Europe. The initiative also includes activities to help startups find international reach. Startups and ecosystem creators have easy access to all financing services and other support offered at EU level.[41]

As shown above, the European Union has made an important qualitative leap in its policy of supporting entrepreneurs through the Startup Europe Project since it was born with a clearly pan-European approach, designing all Member States as a large entrepreneurial ecosystem and not simply as a sum of poles of creativity and isolated talents. It relies on the premise that entrepreneurs and companies linked to digital businesses require a specific management strategy at the European level that leaves startups free to define and develop technologies with more future.[42]

Overcoming excessive localism in the financing and recruitment of talent is a pending issue in the European Union. The national dimension is insufficient, but the Community dimension also seems to be; building bridges with other countries outside the EU around the world and why not with other integration processes, seems to be the current challenge. For example, the Mercosur-EU Association Agreement "in principle" has a special chapter on small and medium-sized enterprises and trade facilitation, which will mean the advancement of trade regulations with the participation of startups.[43]

II.2 The Definition of Data

Considering that the definition of data can be varied, in this work there was a focus on personal data, generally defined as "any information related to an identified or identifiable individual (data subject)".[44]

Although the concept is old, it has become increasingly relevant, because information and communication technologies, especially on the Internet, facilitated the collection of this type of

[39] Kollmann, T., Stöckmann, C., Linstaedt, J. & Kensbock, J. (2015). European Startup Monitor (ESM). German Startup Association. pp 100-102

[40] Scaleup, New: A escalation is a company with an average annualized return of at least 20% in the last 3 years, with at least 10 employees at the beginning of the period.

[41] Belitski, M. & Korosteleva, J. A. (2010). Entrepreneurial Activity Across European Cities. *Frontiers of Entrepreneurship Research*, 30. pp 30-32

[42] Bosma, N. & Schutjens, V. (2011). "Understanding Regional Variation in Entrepreneurial Activity and Entrepreneurial Attitude in Europe". *The Annals of Regional Science*, 47, 711–742. DOI 10.1007/s00168-010-0375-7.

[43] Kollmann, Stöckmann, Linstaedt & Kensbock, op. cit. 2015, pp. 40-45.

[44] Thuret-Benoist, M. (June 27th, 2019*). What is the difference between personally identifiable information (PII) and personal data*? Available at: https://techgdpr.com/blog/difference-between-pii-and-personal-data/

information and, above all, made its management and use economically profitable. It is of high value as a resource for both criminals, authorities and all types of companies, which makes it important to define protection policies for access to this information and the person's own attitude towards partial or total concealment, their reservation for certain purposes or their voluntary assignment.[45]

Under the European Union General Data Protection Regulation (GDPR), personal data is any type of data that can be used to directly or indirectly identify an individual (interested). Some examples of personal data are name, photo, phone number, address (which allow direct identification), as well as IP address or username (which allows indirect identification).[46]

The Organization for Economic Cooperation and Development (OECD) provided the following list of personal data:

- User-generated content, including blogs and comments, photos and videos, etc.
- Activity or behavioral data, including what people search for and view on the Internet, what people buy online, how much and how they pay, etc.
- Social data, including contacts and friends on social networking sites
- Location data, including home addresses, GPS and geographic location, IP address, etc.
- Demographics, including age, gender, race, income, sexual preferences, political affiliation, etc.
- Identification of official data, including name, financial information and account number, health information, national health or social security number, police records, etc. [47]

Some data can be classified under certain parameters, among which:

- Specially protected data: ideology, trade union affiliation, religion, beliefs, racial or ethnic origin, health and sex life.
- Identification data: type and document number, address, image, voice, Social Security/mutual number, telephone, physical marks, first and last name, signature, fingerprint, electronic signature.
- Data on personal characteristics: data on marital status, family data, date of birth, place of birth, age, gender, nationality, physical or anthropometric characteristics.
- Data related to social circumstances: characteristics of accommodation, housing, family situation, property, property, hobbies and lifestyles, membership to clubs and associations, licenses, permits and permits.
- Academic and professional data: training, qualifications, student history, professional experience, participation in schools or professional associations.
- Job details: Profession, jobs, medical support documents, sanctions, evaluations.
- Data that provides business information: Activities and business, business licenses, subscriptions to publications or media, artistic, literary, scientific or technical creations.
- Economic, financial and insurance data: income, income, investments, equity assets, credits, loans, guarantees, bank details, pension plans, retirement, payroll economic data, data on tax/tax deductions, insurance, mortgages, subsidies, benefits, credit history, credit cards.
- Data related to transactions of goods and services: Goods and services, financial transactions, compensation and indemnification.[48]

---

[45] Atzori, L., Iera, A. & Morabito, G. (October 28, 2010). The Internet of Things: A Survey. *Computer Networks*, DOI: 10.1016, *54*, Issue 15, pp. 2787-2805/2787. Available at: http://elsevier.staging.squizedge.net/__data/assets/pdf_file/0010/187831/The-Internet-ofThings.pdf

[46] Bernal, P. (April, 2014). *Internet Privacy Rights*: Rights to Protect Autonomy. Cambridge: Cambridge University Press.

[47] De Hert, P. & Papakonstantinou, V. (August 1, 2015) Comment Google Spain: Addressing Critiques and Misunderstandings One Year Later. *Maastricht Journal of European and Comparative Law*, *22*(4), p. 624.

[48] Atzori & Morabito, op. cit., 2010, pp. 40-60.

In addition to being subject to the application of data protection rules, the processing of personal data may be affected and thus be directly and indirectly regulated by different fields of law, such as competition law, unfair competition law, consumer protection and intellectual property laws.[49]

In this context, it is necessary to favor the use of the principles of data protection and consumer law as a reference to analyze whether there is abuse of dominance under competition rules.[50]

II.3 The Economic Importance of Data

The data and what accompany it, such as analysis, have become a big deal in today's economy.[51] This can also raise many legal, moral and ethical issues, such as cybersecurity, privacy and corporate responsibility for their algorithms.[52] In this sense, startups and large companies are adopting data-driven business models and strategies to gain and sustain a "data advantage" over rivals. This increase, as does the risks of abuse stemming from dominant technology companies.[53]

Given the great commercial and strategic value of personal data, its accumulation (volume and variety), control and use can raise concerns about competition and negatively affect over consumers. It is, therefore, a challenging task to develop a legal framework ensuring an adequate level of protection of personal data while providing an open and more egalitarian field of play for companies to develop innovative data-driven services.[54]

The importance of data in maintaining and supporting competitive digital markets has been widely recognized. In particular, the development of an International Data Strategy[55] aims to free up the power of data for society and the economy at large. At the same time, there is a growing recognition that to get all the benefits of data, consumers must have confidence in the way their data is used.

Exemplifying, in the UK, the Data Ethics and Innovation Centre was created by the government in 2018, to provide advice on measures enabling safe, ethical and innovative use of data-driven technologies.[56] It is currently analyzing the use of data to shape people's online experiences and the potential for bias in algorithmic decision-making. A parallel government analysis of smart data is

---

[49] Hildebrandt, M. (2009). Privacy and Identity. In: E. Claes, A. Duff & S. Gutwirth (eds) *Privacy and the criminal law*. Antwerp/Oxford: Intersentia. pp. 61-104.

[50] Bernal, op. cit., 2014, pp 20-24.

[51] It is the protection of computer systems against theft or damage to hardware, software or electronic data, as well as the interruption or disorientation of the services they provide.

[52] Monteleone, S. & Puccio, L. (January 19, 2017). *From Safe Harbour to Privacy Shield*: Advantages and shortcomings of the new EU-US data transfer rules. European Parliamentary Research Service.

[53] Carnevale, S. G. (2018). *Europe's new data protection rules export privacy standards worldwide*. https://www.politico.eu/article/europe-data-protection-privacy-standards-gdprgeneral-protection-data-regulation/

[54] Hustinx, P. (July 1-12, 2013). *EU Data Protection Law*: The Review of directive 95/46/EC and the Proposed General Data Protection Regulation. Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law.

[55] Blume, P. (2014). The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law*, *4*(4), pp. 269-273.

[56] Data Ethics and Innovation Consultation Centre. (November 20, 2018). Available at: https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation

exploring how data portability can improve the consumer experience in regulated utility markets through the use of innovative intermediaries and other services.[57]

II.4 Data in the Digital Single Market

Digitization has shaped and influenced the business world for years. Some industries are more successful than others in taking advantage of digitization through new strategies. One of the industries that has by no means exhausted its potential in this sense is physical retailing. Traditional European retailers are still in the early stages of using digital technologies and providing digital services to their customers, although many technologies are marketable.[58]

Many scanning potentials are widely known, but are rarely implemented in practice. In addition to increasing the competitive pressure of online commerce, transforming classic business models into digital business models presents major challenges for the entire market. Not only is consumer shopping behavior changing, business sales activities are also changing.[59]

As digitization is advancing, data is also becoming increasingly important to the economy at large. Due to the mass and possible uses, a data market has already formed and those who own them have the decisive advantage of being able to use them for various purposes at the same time, which even includes negotiating their sale.[60]

In 2015, the European Commission said it was actively investigating Google's activities, including whether the technology company illegally prevented the development and market access of rival mobile apps or services by requiring or encouraging smartphone and tablet manufacturers to exclusively pre-install Google's own applications or services.[61]

In the EU, competition, consumer and data protection laws share common objectives. These three legal areas aim to protect the general public (consumers) and contribute to the functioning of the internal market, and in particular the digital single market. However, the means by which these objectives are pursued differ.[62] Article 3 of the Treaty on the functioning of the European Union makes it clear that the establishment of the EU internal market includes "a system ensuring that competition is

---

[57] Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), pp. 68-92.

[58] Knapp, A.-K., Marchand, A. & Hennig-Thurau, T. (2017). How to survive in a digital world? A comprehensive analysis of success factors for brick-and-mortar retail stores: an abstract. In: M. Stieler (Hrsg.). *Developments in marketing science*: proceedings of the Academy of Marketing Science, Creating Marketing Magic and Innovative Future Marketing Trends, 2016. Academy of Marketing Science (AMS) Annual Conference (S. 31). New York: Springer. pp. 50-55.

[59] Lemke, C., Brenner, W. & Kirchner, K. (2017). *Einführung in die Wirtschafts informatik*. Berlin, Heidelberg: Springer. pp. 10-12.

[60] Hagberg, J., Jonsson, A. & Egels-Zandén, N. (2017). Retail digitalization: implications for physical stores. *Journal of Retailing and Consumer Services*, (39), pp. 264-269.

[61] European Commission. (April 15, 2015). *Antitrust*: Commission sends statement of objections to Google in the shopping comparison service (MEMO/15/4781). Brussels. Available at: http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm

[62] European Commission. Id.

not distorted".[63] Moreover, article 101(1) [64] of the Treaty prohibits agreements between undertakings, decisions of associations of undertakings and concerted practices which may affect trade between Member States, and which have the objective or effect of preventing, restricting or distorting competition in the internal market.

II.5 "Data Power" and Market Power

Considering the inherent characteristics of data collecting, the concentration of economic power is obvious. Every day it is observed how the largest companies in the economy increase their influence. Data is increasingly influencing competitiveness among companies, especially in terms of revenue generation through direct use of data, for example through advertising or in terms of improving data-driven products and services. In this sense, the company that owns them also has an advantage over its competitor that does not have such data.[65]

Competitive advantage means, from an economic point of view, an advantage over competition in the market. Such competitive advantage can be divided into a provider advantage and a customer advantage. For a company, a competitive advantage means that it is always at least one step ahead of others undertakings. For all companies, competitive advantage is the key to sustainable corporate success. In the long run, a company can only generate a profit surplus if it has a qualitative advantage over its competitors. A competitive advantage for a company arises from entrepreneurial and strategic actions, and can be factors such as prices, special sales characteristics, or flexible production models.[66]

Furthermore, genuine unfair advantages[67] are important factors that allow the customers to offer a significantly better product than their competitors - which are difficult to copy by others - even if they have much more capital (a likely scenario).

In practical terms of unfair advantages, one can retain knowledge that the competition does not have, taking advantage of it to provide better products than the competition. For example, privileged

---

[63] Official Journal of the European Union. (Outubro 26, 2012). *Consolidated version of the treaty on the functioning of the European Union* (C 326/390). Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF

[64] Abreu, J. C. (2019). The design of electronic justice Europe from 2019 to 2023 in the light of the Union litigation. *Anticipatory Reflections,*

[65] Kaisler, S., Armour, F., Espinosa, J. A. & Money, W. (Jan. 7-10, 2013). Big Data: Issues and Challenges Moving Forward. In: *Proceedings of the 46th Hawaii International Conference on System Sciences*, DOI: 10.1109/HICSS.2013.645, IEEE: 13385077, pp. 995-1004. Available at: https://ieeexplore.ieee.org/document/6479953

[66] Madden, S. (May-June 2012). *From Databases to Big Data*, Massachusetts Institute of Technology, DOI: 10.1109/MIC.2012.50. *16*, pp. 4-6. Available at: http://www.computer.org/csdl/mags/ic/2012/03/mic2012030004.pdf

[67] Kaisler, Armour, Espinosa, & Money, ibid., 2013, pp. 14-16.

market information about price or demand model (e.g. Uber) or even data about the user's consumption preferences, divided by gender, country etc. (e.g. Netflix).[68]

It is necessary to unify, or even to provide the main factors identifying the power related to the data. This leads to a new unit, which relies on experts and deals only with the data market, at an international level, or at least at the European Union level to begin with. This unit needs to understand the innovation process and how exactly and deeply this fast-growing world of startup and technology works, favoring and encouraging competition, protecting the underprivileged undertakings, such as startups.[69]

[68] Zikopoulos, P.C., Eaton, Ch., Deroos, D., Deutsch, T. & Lapis, G. (2012*). Understanding Big Data*: Analytics for Enterprise Class Hadoop and Streaming Data. The McGraw-Hill Companies.

[69] Madden, op. cit., 2012, pp. 10-14.

III. COMPETITION LAW

Competition law is a law field that lays down rules and procedures aimed at protecting free competition on the market. Competition law usually exists in countries operating under a market economy system, where companies and individuals are free to start or terminate a commercial business for profit.[70] In another definition, competition law is the branch of law that regulates trade, prohibiting illegal restrictions, prices and monopolies. It aims to promote competition between existing companies in a market and promote the quality of goods and services at the lowest possible price, ensuring an efficient market structure.[71]

The aim of competition law is to promote "fair competition" between companies. It had a great effect on commercial practices and in restructuring the industrial sector in countries. Based on the premise that free trade benefits consumers, businesses and the economy in general, the law prohibits different types of trade restrictions and abuse of monopolization.[72]

From a general point of view, these restrictions can be of four different types: horizontal agreements between competitors, vertical agreements between buyers and sellers, abuse of dominant position (monopoly) and mergers. European law also prohibited State aid, thereby considered a violation of competition law.[73]

In a free market system, there is confidence that free trading between buyers and sellers will be the best system to achieve efficiency. However, it is acknowledged that, on some occasions, it is necessary for the State to intervene to prevent and punish conduct aimed at limiting competition.[74] Nevertheless, the goal of Competition Law is to preserve an ideal environment for companies and individuals to compete freely and on their own merits.[75]

Among the elements considered by competition law, there are the following:

a) Creation of authorities responsible for protecting free competition in the market. Its structure, mission and powers are usually defined.
b) Definition, prosecution and sanctioning conducts that considered anti-competitive.
c) Establishment of procedures for requesting investigation, sanction and compensation.

---

[70] Veni, J.S. (1996). EU Competition Law-Enforcement and Compliance: An Overview. *Antitrust Law Journal*, *65*, pp. 81-104.

[71] Wilks, S. (June 13, 2005). Agency Escape: Decentralization or Dominance of the European Commission in the Modernization of Competition Policy? *Governance*: An International Journal of Policy, Administration, and Institutions, DOI: 10.1111/j.1468-0491.2005.00283.x, *18*(3), pp. 431-452.

[72] Weiss, F. (2006). Transparency as an element of good governance in EU and WTO practice: overview and comparison. *Fordham International Law Journal*, *30*, pp.1545-1586.

[73] Veni, ibid., 1996, pp. 10-12.

[74] Wilks, ibid., 2005, pp. 20-22.

[75] Teacher, L. (2013). *Competition Law Dissertation Topic Examples*. Available at: https://www.lawteacher.net/law-dissertation-topics/competition-law.php?vref=1

III.1 Origins of Competition Law

At the end of the 19th century, capitalism in industrialized countries was questioned by much of society. In the case of the USA, the traditional interpretation considers that the criticisms were directed mainly at the huge conglomerates of companies, the so-called trusts (where the name antitrust comes from). These conglomerates included competing companies, which were part of the trust. They could establish and raise the price of their products together, leading to dissatisfaction and complaints from consumers and farmers.[76]

Another interpretation considers that small businesses pressured the government to intervene, because they were unable to compete with trusts' lower prices. According to this version, small businesses would not have been able to compete with the efficiencies resulting from large-scale production (which in economic jargon is known as "economies of scale") and would have lead the government to protect them. While it is true that during this period, many products, such as gasoline, suffered price falls of up to 80% between 1860-1903. Nevertheless, it would be difficult to prove that such falls had not yet occurred as consequence of trust relationships.[77]

Moderate opinions consider that consumers and small businesses had put pressure on the government in the same way. In the case of small businesses, they claimed that trusts imposed predatory prices (prices below cost) to eliminate the formers and subsequently increased prices when competition was eliminated, or even prevented other companies from entering the market, reducing competition.[78]

Anyway, as a result of the discussion about monopolies, the Sherman Antitrust Act was created in 1890. The US Senator John Sherman presented the bill, which is considered the birth of current antitrust legislation. Subsequently, Congress repeatedly amended the law during the 1950s and, therefore, the set of laws that make up the current antitrust law.[79]

III.2 Competition Law According to the EU

The European development in competition law is considerable different from the American law. Some authors argue that the European antitrust model was first articulated in Austria at the end of the

[76] Weiss, op. cit., 2006, pp. 50-90.

[77] Wils, W.P.J. (2008). The Use of Settlements in Public Antitrust Enforcement: Objectives and Principles. *World Competition*, *31*(3), pp.335-352.

[78] White, S. (2009). Rights of the Defense in Administrative Investigations: Access to the File in EC Investigations. *Review of European Administrative Law*, *2*, Issue 1, pp. 57-69.

[79] Zingales, N. (2010). The Hearing Officer in EU Competition Law Proceedings: Ensuring Full Respect for the Right to Be Heard? *Competition Law Review*, *7*, Issue 1, pp.129-156.

19th century (from where it was implanted in the rest of Europe) and was born as a rejection of the American model.[80]

In any case, European countries began to genuinely interest in antitrust measures later than in the US, as European companies were smaller and therefore the risk of cartelization or abuse was much lower. It was not until the 20th century that individual countries began to develop their own antitrust laws. The Treaty of Rome in 1957 assumed the creation of the European Economic Community.[81]

Since then, economic integration and the creation of the single market have been promoted. A process of liberalization and privatization of companies that is still valid today has also begun. Thus, mergers were fostered between companies (national or European) and, therefore, the emergence of larger companies. Thus, European interest in antitrust law has grown.[82]

Currently, the exercise of Competition Policy in the European Union is regulated by Regulation 1/2003, (which entered into force in 2004). It establishes, firstly, in which cases it is up to the European or national authorities to act. In general, cases affecting the trade of the Member State are the responsibility of only the national authorities (this criterion is specified in that Regulation), with the European authorities reserving cases affecting more than one Member State.[83]

Secondly, it allows each Member State to maintain its own laws, as long as they are not contrary to European Community law. This last point would encourage innovation, for example by creating new rules that did not exist, from the different European agencies.[84]

III.3 The Economic Theory of Competition

Competition refers to the struggle for (or maintenance of) commercial superiority. In the commercial world, this involves the effort to get as many customers as possible. In the United Kingdom, the Competition Commission describes competition as "a process of rivalry between companies, in order to obtain customers".[85]

In general, the greater the competition, the more likely companies are to be efficient (and therefore lower their prices) and the greater the varieties or types of products (both in quantity and

[80] Zhang, A.H. (2011). Problems in Following E.U. Competition Law: A Case Study of Coca-Cola/Huiyuan. *Peking University Journal of Legal Studies*, The University of Hong Kong - Faculty of Law, *3*, pp. 96-118. Available at: http://ssrn.com/abstract=1569836

[81] Wils, op. cit., 2008, pp. 7-9.

[82] Teacher, op. cit., 2013, pp. 100-104.

[83] White, op. cit., 2009, pp. 54-90.

[84] Zingales, op. cit., 2010, pp. 70-74.

[85] Teacher, op. cit., 2013, pp. 90-99.

quality). In this sense, there are different situations or degrees of competition that may exist in a market, as follow.[86]

Perfect competition is the situation in which the market is most competitive possible: all agents are price takers (price makers) and therefore have no power to influence prices, obtaining companies the minimum benefit necessary to maintain production. If one company obtains surplus profits, another will enter the market until prices and profits return to the previous level.[87]

In the case of the perfect competition practically theoretical, most markets are deemed as some form of imperfect competition. In this case, the number of companies on the market is lower than in the case of perfect competition (e.g. in the case of oligopoly, with few companies, or duopoly, with only two companies). For this reason, companies in such a situation have some power over prices and are able to obtain surplus profits.[88]

Imperfect competition may also be due to barriers to entry, preventing the increase in the number of competitors (due to the intrinsic characteristics of the market or some state intervention that prevents entry into that market, for example by means of a patent).[89]

The less competitive market situation is that of a monopoly, in which there is only one company that offers a particular product without consumers having an alternative (for example, a company that dominates between 50% and 100% of the market). In this case, the company receives high benefits because it can set the price with greater freedom, that is, it is a price determiner.[90]

In the case of few companies in the market (oligopoly), there is the possibility of them acting as a monopoly, by collusion in a cartel or by parallel behavior. Even so, the fact that a single company exists on the market does not imply that it has market power (or pricing power) if that market is a contestable market. In a contestable market, a company can only remain monopolistic if it produces as efficiently as possible and/or does not generate excessive profits. If the company became inefficient or made excessive profits, another company would enter the market and dominate it.[91]

---

[86] Kochar, P. (2009). *Critically assess the way in which Article 102 TFEU has been modernised,taking as a case study the enforcement of Article 102 TFEU against either Microsoft, Intel or Google*.

[87] Decker, C. (2009). *Economics and the Enforcement of European Competition Law*. Research Fellow in Law and Economics, CSLS, University of Oxford, UK: Mr. Edward Elgar Publishing. Cheltenham. pp. 10-12.

[88] Mușetescu, R., Dima, A. & Păun, C. (2008). *The Role of the Competition Policy in Forging the European Common Market*. Munich Personal RePEc Archive. University Library of Munich. Germany. pp. 22-30.

[89] Röller, L.-H. (2005). *Economic Analysis and Competition Policy Enforcement in Europe in Modelling European Mergers*: Theory, Competition and Case Studies.: Edward Elgar. pp. 18-40.

[90] Kochar, op. cit., 2009, pp. 20-25.

[91] Papadopoulos, A. (2010). *The International Dimension of EU Competition Law and Policy*. The UK: Cambridge University Press. pp 25-27.

In conclusion, the degree of competition in a market can vary markedly according to its characteristics.[92] Without intending to make this list complete, the following items are considered "unfavorable elements of competition":

a) The presence on the market of a small number of competing companies.
b) High market shares for companies present in the market (for example, if there are still any companies, only two dominate 80% of sales in the market).
c) The existence of barriers to entry.
d) A reduced elasticity of demand (i.e. a situation where an increase in prices has not substantially reduced the company's sales, making this increase profitable for the company and thus encouraging the company to increase prices).

[92] Zhang, op. cit., 2011, pp. 44-60.

III.4 Objectives of Competition Law

From a theoretical point of view, the ultimate goal of competition law is to maximize the consumer's surplus, which implies the lowest possible prices so that consumers can purchase a greater number of products and varieties.[93]

However, reality is more complex and other goals have been attempted through competition, with the law sometimes trying to achieve opposite goals.[94] The following objectives can be cited:

a) Consumer law.

b) Redistribution.

c) Protection of competitors.

d) Supplier protection.

e) Single market (in the case of the European Union).

These objectives need a comprehensive analysis, as follows.

III.4.1 Consumer protection

While there is a more or less widespread consensus that the main objective of competition law should be to maximize consumer welfare, there is no consensus as to the manner or means by which to achieve those objectives. In the opinion of many lawyers and economists, this consumer well-being must be achieved by protecting the competitive process and not the consumer itself.[95]

A typical example of this concern is excessive price jurisprudence: for many years, plaintiffs attempted to use competition laws in Courts, in order to accuse companies of setting excessively high prices.[96]

The problem with using competition law to take direct control of corporate prices is that the regulator is usually in a bad position to determine whether the price would be in a competitive market or not.[97] Adding, it is necessary to know the cost curves of companies, market demand and other

[93] Stylianou, K. (2016). *Help Without Borders*: How the Google Android Case Threatens to Derail the Limited Scope of the Obligation to Assist Competitors. University of Leeds, School of Law. pp. 90-99.

[94] Teacher, op. cit., 2013, pp. 68-90.

[95] Anderson, R. & Jenny, F. (2005). Competition Policy, Economic Development and the Role of a Possible Multilateral Framework on Competition Policy: Insights from the WTO Working Group on Trade and Competition Policy. Chapter 4'. In: E. Medalla (ed.). *Competition Policy in East Asia* (pp. 61-85). UK: Routledge.

[96] Röller, op. cit., 2005, pp. 77-103.

[97] Stylianou, op. cit., 2016, pp. 16-88.

aspects, in order to judge objectively the conducts. Furthermore, such calculation is highly complicated. In fact, by setting a price, the regulator may end up causing more distortions than it tries to alleviate.[98]

III.4.2 Redistribution

At times, objectives have been pursued that have more to do with promoting a fair economy than with an efficient economy. For example, the attempt to reduce the accumulation of resources in large companies and conglomerates, as regarded as a threat to democracy itself.[99]

III.4.3 Protection of competitors

The protection of competitor perspective considers that competition should be applied in a way that protects small competitors from stronger rivals, seeing its objective as intrinsic to the protection of the competitive process.[100]

The problem with this way of looking at the competition is that by protecting the smaller undertaking, you can reward the inefficient company and punish the efficient one, because if the later can establish lower prices, eliminating its lower competitors, this will certainly occur because it has lower costs or cost-margins when compared with the former.[101]

III.4.4 Single Market: the European case

In the European case, competition policy has played a very important role in achieving the so-called single market, i.e. in the economic integration of the different markets of the Member States, for example through the growth of trade, increase in companies of a European (and not just national) nature, convergence of intellectual property rights etc.[102]

For example, in 2002, in the case of Nintendo, the European Commission imposed a fine of EUR 167.8 million on Nintendo for preventing the export of video game consoles from the United Kingdom to Germany and the Netherlands.[103]

---

98 Decker, op. cit., 2009, pp. 54-67.
99 Mușetescu, Dima, & Păun, op. cit., 2008, pp. 99-107.
100 Papadopoulos, op. cit., 2010, pp. 87-98.
101 Kochar, op. cit., 2009, pp. 76-80.
102 Stamate, A. (2011). On Some Economic Aspects of the European Competition Policy Rhetoric. *Romanian Economic and Business Review*, *6*, Issue 3, pp. 127-137.
103 Kochar, op. cit., 2009, pp. 78-80.

In this case law, the goal of companies that use these strategies is to segment each national market to impose different prices in different countries. If, for example, in the UK, a gaming console is sold cheaper than in Germany, the producer prohibits its distributors from exporting them to that country or even selling them to exporters.[104] Thus, the company guarantees that it can impose the highest price allowed by the elasticity of demand in each country (in this case, it is assumed that the elasticity would be higher in the United Kingdom than in Germany, because in the first prices were lower).[105]

This type of behaviour has been prosecuted by the Commission and banned by the European Court of Justice on several occasions in order to consolidate the European Single Market, making this case law part of the doctrine known as parallel trade.[106]

According to the Court's decision, traders can export or import goods from other countries to take advantage of price differences (which sometimes allow large profits). This is how companies are pressured to have a single price policy at European level, with price convergence being the ultimate goal of the single market.[107]

III.5 European Institutions Responsible for Competition Law

The main institutions responsible for the implementation and revision of competition rules in the European Union are:

a) The European Commission.

b) The European Court of First Instance.

c) The Court of Justice of the European Union (ECJ).

These institutions have relevant roles in EU Competition law, as shown below.

[104] Anderson, & Jenny, op. cit., 2005, pp. 70-90.
[105] Zingales, op. cit., 2010, pp. 78-90.
[106] Stylianou, op. cit., 2016, pp. 90-99.
[107] Stamate, op. cit., 2011, pp. 100-102.

III.5.1 European Commission

The European Commission is the executive power of the EU. It also has the exclusive legislative initiative on competition, i.e. it is the only one with the authority to propose regulations in this area (which must be subsequently approved by Parliament and the European Council).[108]

In addition, it is responsible for ensuring compliance with the rules and, in the case of competition rules, this implies ensuring that the behaviour of companies does not violate the laws. In the event that you find that they violate them, you are the only one with the power to take the accused companies to court. It should also be noted that, in terms of mergers, it is responsible for admitting or prohibiting them (with the possibility of appealing against that decision in court).[109]

III.5.2 The Lisbon Treaty

For the first time, the Lisbon Treaty defined the distribution of competences between the EU and the Member States in the areas of research, technological development and space as a shared competence.

A new protocol stated that the Union may take action under Article 308 to ensure free and undistorted competition in the internal market.

The Lisbon Treaty also suppressed the 50-year-old commitment to "undistorted competition", embedded in the fundamental provisions of the EC Treaty (Article 3(1)(g) EC). Since the Lisbon Treaty came into force on December 1, 2009, there has been no Treaty provision proclaiming adherence to the principle of undistorted competition. The substantive content of Article 3(1)(g) EC has been transferred to a Protocol (No 27) on the Internal Market and Competition, annexed to the Treaties.

With this new treaty, some changes occurred, mainly in the jurisdictional system of the European Union: the previous "Court of Justice of the European Community" was changed to the new Court of Justice of the European Union that now includes: the Court of Justice, the General Court and specialised courts (Article 19 TEU).

The Court of Justice of the European Union (which sometimes is also referred to as the European Court of Justice), constitutes the highest judicial authority of the EU. It ensures, in

---

[108] Crandal, R.W., & Winston, C. (2005), 'Does Antitrust Policy Improve Consumer Welfare? Assessing the Evidence', Chapter 2. In: C. Robinson (ed.). Governments, Competition and Utility Regulation (pp 109-200) London Business School, The Institute of Economic Affairs, Cheltenham: Edward Elgar Publishing Limited.

[109] Baker, J.B. (2003). The Case for Antirust Enforcement. *Journal of Economic Perspectives*, *17*(4), pp. 27-50.

cooperation with the courts and tribunals of the Member States, the application and uniform interpretation of European Union law. Also, is composed of one judge from each Member State.

The General Court hears cases in first instance, which are not referred to the specialised courts or directly to the Court of Justice. It also deals with appeals against decisions (of first instance) made by the European institutions, namely the European Commission, in competition matters.

Specialised courts can be set up for specific areas. They can hear and determine cases at first instance, with the possibility of an appeal to the General Court.

Based on that structure, Apple contested, before the General Court, a Commission Decision (EU) regarding "distort competition".

III.5.3 European Competition Law

European competition law can be subdivided into the following blocks, which correspond to different articles of the Treaty of Rome and the European Merger Regulation: [110]

a) Council Regulation (EC) No 1/2003: defines in what situations and how competition law should be applied.
b) Article 101 TFEU: prohibiting cartelisation.
c) Article 102 TFEU: prohibiting abuse of a dominant position.
d) Article 106 TFEU: prohibition of State aid.
e) European Merger Regulation: regulate the notification and admission or prohibition of mergers and acquisitions at European level.

[110] Böge, U. (December 9, 2003). *Antitrust Enforcement in Europe*: The New Challenges (Merger Control). With a particular Focus on the Examination of Minority Interests under the German Merger Control Regime. (Speech at the Italian Competition Day). Rome, Italy. Available at: http://www.agcm.it/AGCM_ITA/EVENTI/EVENTI.nsf/cd33e4d549490cb4c12569 9000386c4c/37d3dc946f3f4716c1256dff005fc0ef/$FILE/UB.pdf

III.6 Council Regulation (EC) No. 1/2003

Council Regulation (EC) No 1/2003 establishes the framework in which competition law, in particular Articles 81 and 82, should be applied to all EU members.[111] First, Council Regulation (EC) No 1/2003 refers to its task of creating a "network of national authorities"[112] to cooperate in the application of competition law at European level:

> §15: The Commission and the competition authorities of the Member States shall form together a network of public authorities applying Community competition rules in close cooperation. To do this, you need to create information and query mechanisms. The Commission, in close cooperation with the Member States, will establish and analyse additional details of cooperation in the network.[113]

The Council Regulation (EC) No 1/2003 also distinguishes that the burden of proof of infringement falls on the private party or administration alleging it and which corresponds to the undertaking accused of proving that efficiencies exist within the meaning of Article 81.3:

> Article 2: In all national and Community procedures for the application of Articles 81 and 82 of the Treaty, the burden of proof of a breach of Article 81(1) or Article 82 of the Treaty in the part or authority alleging it. The undertaking or association of undertakings which it invokes in accordance with Article 81(3) of the Treaty shall prove that the conditions laid down in that paragraph are fulfilled.[114]

It is also established that national law may not be contrary to the provisions of the Treaty, i.e. that national rules may not be contrary to European standards, but may go beyond those, i.e. more restrictive than the previous ones:

> Article 3.2: The application of national competition law may not result in the prohibition of agreements, decisions or associations of undertakings or concerted practices which may affect trade between Member States but do not restrict competition within the meaning of Article 81. (1) of the Treaty or which fulfil the conditions of Article 81(3) of the Treaty or which are covered by a regulation implementing the Treaty. The provisions of this Regulation shall not prevent Member States from adopting and enforcing stricter national laws in their respective territories, whereby certain behaviours adopted unilaterally by undertakings are prohibited or punished.[115]

---

111 Official Journal of the European Communities. (December 16, 2002). *Council Regulation (EC) No 1/2003 of 16 December 2002*, on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003R0001&from=EN

112 Official Journal of the European Communities, id. a

113 Official Journal of the European Communities, id. b

114 Official Journal of the European Communities, id. c

115 Official Journal of the European Communities, id. d

In addition to these provisions, Council Regulation (EC) No 1/2003 refers to the forms of relationship between the European Commission and national administrations.[116] To that end, it is established that national decisions should not be contrary to Commission decisions.

> Article 16: 1. Where national courts decide on agreements, decisions or practices pursuant to Articles 81 or 82 of the Treaty which have already been the subject of a Commission decision, they may not adopt resolutions incompatible with the decision adopted by the Commission. They should also avoid taking decisions that may conflict with a decision envisaged by the Commission in the procedures already initiated. To this end, it is up to the national courts to assess whether to suspend their procedures. This obligation must be understood without prejudice to the rights and obligations set out in Article 234 of the Treaty. 2. Where the competition authorities of the Member States decide agreements, decisions or practices pursuant to Articles 81 or 82 of the Treaty which have already been the subject of a Commission decision, they may not take decisions incompatible with the decision taken by the Commission.[117]

[116] Official Journal of the European Communities, id. e
[117] Official Journal of the European Communities, id.

IV. DATA PROTECTION AND COMPETITION LAW IN THE EU

IV.1 Data Protection Overview

Data protection is a legal discipline that deal with the danger posed by the indiscriminate collection and use of personal data, understanding as similar to all information that is an integral part of our private sphere and that can be used to assess certain aspects of our personality (habits, personal relationships, opinions).[118]

The data protection solution is a series of rules designed to limit the use of personal data, thus ensuring the honor of citizens. It covers all types of processing of personal data (regardless of whether they are carried out manually or computerised), calculating, allowing the collection, using and transmitting information.[119]

One of the main principles of data protection is that personal data can only be collected for processing purposes, submitting them when convenient, relevant and not excessive in relation to the field and the objectives determined. In addition, a legal provision makes it clear that the processing of the data will require the permission of the injured party. Persons who intervene at any stage of the processing of personal data have an obligation to maintain professional secrecy.[120]

IV.2 General Data Protection Regulation (GRPD)

The GDPR establishes specific requirements for companies and organizations regarding the collection, storage, and management of personal data. They apply both to European organisations that process personal data of citizens in the EU and to organisations based outside the EU and whose activity is directed at people living in the EU.[121] This is applied in the following situations:

a) The company processes personal data and is based in the EU, regardless of where the data is actually processed.

b) The company is based outside the EU, but processes personal data about offers of goods or services to EU citizens or monitors the behaviour of citizens in the EU.[122]

---

[118] Kennedy, J. (March 2017). *The myth of data monopoly*: why antitrust concerns about data are exaggerated. Information Technology & Innovation Foundation. Available at: http://www2.itif.org/2017-data-competition.pdf

[119] Koščík, M. (2016). *The Impact of General Data Protection Regulation on the grey literature*, *13*, pp. 42-46.

[120] Žák, Č. (2017). *When preparing for GDPR, do not forget to insure*. ICT Revue. p. 32.

[121] Kennedy, op. cit., 2017, s/p.

[122] Kennedy, id.

EU data protection rules ensure the protection of personal data in all cases where it is collected: for example, when buying online, submitting a job application or applying for a bank loan.[123]

These rules apply to companies and organizations (public and private) based in the EU and those based outside the EU and offering goods and services in the EU, such as Facebook or Amazon. The rule is applicable to companies request or reuse personal data from EU citizens.[124] It doesn't matter the format in which the data is collected (online, on a central computer, or on paper, in a structured file); whenever the information directly or indirectly identifies an user as an individual, while is stored or processed information, her data protection rights must be respected.[125]

IV.2.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the European Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data. It entered into force on 25 May 2016 and was applicable on 25 May 2018, two years during which companies, organizations, agencies and institutions were adapting to compliance.[126]

Moreover, it is a regulation at European Union level. Therefore, any union company, or those doing business in the European Union, dealing with personal information of any kind, must use it. Fines for non-compliance with the GDPR can reach EUR 20 million.[127]

---

123 Tantleff, A. K. (2017). Equifax Breach Affects 143M: If GDPR Were in Effect, What Would Be the Impact? *Journal of Health Care Compliance*, *19*(5), pp. 45-46. Available at: http://escweb.lib.cbs.dk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&A N=126012049&site=ehost-live&scope=site

124 Sobolewski, M., Mazur, J., Paliński, M. (August 10, 2017). GDPR: A step towards a user-centric internet? *Intereconomics*, DOI: 10.1007/s10272-017-0676-5, *52*(4), pp. 207-213. Available at: https://link.springer.com/article/10.1007/s10272-017-0676-5

125 Goddard, M. (November 1, 2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, DOI: 10.2501/IJMR-2017-050, *59*(6), p. 703. Available at: https://journals.sagepub.com/doi/10.2501/IJMR-2017-050

126 Carnevale, op. cit., 2018, s/p.

127 Koščík, op. cit., 2016, s/p.

In Spain, the GDPR made obsolete the Organic Law on the Protection of Personal Data (LOPD) of 1999, being replaced on December 6, 2018 by the Organic Law on the Protection of Personal Data and guarantee of digital rights, according to the GDPR.[128]

IV.2.1.1 Scope

The referred regulation applies whether to the data controller (an organization that collects data from EU residents) or to the processor (an organization that processes data on behalf of the data controller, for example, cloud service providers) or to the data subject (person) is based in the EU. In addition, the Regulation also applies to organizations based outside the European Union if they collect or process personal data from EU residents. In terms of personal data, according to the European Commission,

> personal data is any information relating to an individual, whether relating to his or her private, professional or public life. They can be anything from name, address, photo, email address, bank details, posts on social media sites, medical information or the IP address of a computer.[129]

The Regulation does not apply to the processing of personal data for national security or law enforcement activities in the European Union; however, industry groups concerned about facing a potential conflict of laws questioned whether Article 48 of the GDPR could be invoked to prevent a data controller subject to the laws of a third country from complying with a law enforcement order. National security authorities shall disclose to those authorities the personal data of an EU person, regardless of whether the data resides within or outside the EU.[130]

Article 48 states that any judgment of a court and any decision of a third-country administrative authority requiring a controller or processor to transfer or disclose personal data may only be recognized or enforced in any way if based on an international agreement, such as a mutual legal assistance treaty in force between the requesting third country (outside the EU) and the Union or a Member State , the data protection reform package also includes a separate data protection directive for the police sector and the justice system laying down rules for the exchange of personal data at national, European and international levels.[131]

[128] Carnevale, op. cit., 2018, s/p.
[129] Koščík, op. cit., 2016, s/p.
[130] European Commission, 2016.
[131] Sobolewski, Mazur, & Paliński, op. cit., 2017, s/p.

IV.2.1.2 Single set of rules and single window

A single set of rules will apply to all EU member states. Each Member State shall establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offences, etc. The SAs of each Member State will cooperate with other SAs, providing mutual assistance and organizing joint operations.[132]

When a company has several establishments in the EU, it will have a single SA as its "main authority", depending on the location of its "main establishment" (i.e. the place where the main treatment activities are carried out). The lead authority will act as a "one-stop shop" to oversee all treatment activities of that company across the EU. The European Data Protection Council (EDPB) will coordinate SA. The EDPB will replace the Article 29 Working Group.[133]

There are exceptions to data processed in an employment context and data for national security purposes that may still be subject to each country's regulations.[134]

IV.2.1.3 Responsibility

In the EU regulation, notification requirements remain and expand. However, they should include the retention time of personal data and contact information of the data controller and a data protection officer must be provided.[135]

Automated individual decision-making, including profiling (Article 22), is debatable, similar to the Data Protection Directive (Article 15). In this case, citizens have the right to question and combat important decisions that affect them and that have been made solely based on the algorithm. Many media outlets have commented on the introduction of a "right of explanation" algorithmic decisions but since jurists argue that the existence of such a right is not very clear without a judicial trial and, at best, is limited.[136]

In order to demonstrate GDPR compliance, the data controller must implement measures that comply with the principles of data protection by design and data protection by default. Then, privacy by design and by default (Article 25) requires data protection measures to be designed for the

[132] Zarsky, Tal Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, *47*, Iss. 4, p. 995.
[133] Tantleff, op. cit., 2017, s/p.
[134] European Commission, 2016.
[135] Goddard, op. cit., 2017, s/p.
[136] Kennedy, op. cit., 2017, s/p.

development of business processes for products and services. Such measures include the pseudonymization of personal data by the controller as soon as possible (recital 78).[137]

It is the responsibility of the data controller to implement effective measures and be able to demonstrate compliance with processing activities, even if processing is performed by a data processor on behalf of the controller.[138]

Adding, in terms of data protection impact assessments (Article 35), it should be carried out when specific risks to the rights and freedoms of data subjects occur. The reason why is risk assessment and mitigation is required and prior approval by Data Protection Authorities (DPA) is necessary for the highest risks. Therefore data protection officers (Articles 37 to 39) must ensure compliance in organizations. The EU Commission designated the following classification:

a) For all public authorities, except for courts acting in their judicial capacity;
b) If the main controller or processor activities consist of:
    i) Treatment of "operations" that, due to their nature, scope and/or purposes, require regular and systematic control of stakeholders on a large scale;
    ii) Processing on a "scale" large specific categories of data pursuant to Article 9 and personal data relating to criminal convictions and crimes provided for in Article 10.[139]

IV.2.1.4 Legal basis for treatment

Data can only be processed if there is at least one legal basis for this. The legal bases for data processing are:

a) The interested party has given its consent to the processing of your personal data for one or more specific purposes.
b) Treatment is necessary for the performance of a contract to which the interested party is a party or to take action at the request of the interested party before concluding a contract.
c) Treatment is necessary to comply with a legal obligation to which the controller is subject.
d) Processing is necessary to protect the vital interests of the data subject or other natural person.
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority conferred on the controller.

[137] O'Brien, R. (June 8, 2016). Privacy and security: The new European data protection regulation and its data breach notification requirements. *Business Information Review*, DOI: 10.1177/0266382116650297, *33*(2), pp. 81-84. Available at: https://journals.sagepub.com/doi/10.1177/0266382116650297
[138] Sobolewski, Mazur, & Paliński, op. cit., 2017, s/p.
[139] European Commission, 2016.

f) Processing is necessary for the legitimate interests of the controller or third parties, except where those interests are replaced by the interests or fundamental rights and freedoms of the interested party requiring protection of personal data, especially where the interested party is a child.[140]

IV.2.1.5 Consent

When consent is used as a legal basis for processing, consent must be explicit for the data collected and for the purposes for which the data is used (Article 7, defined in Article 4). The consent of the children must be given by the child's parents or guardian and verifiable (Article 8). Data controllers should be able to test "consent" (acceptance) and consent can be withdrawn.[141]

The issue of GDPR consent has several implications for companies that record calls in practice. Typical "This call is being recorded for security reasons" warnings will no longer be sufficient to obtain the consent assumed to record calls. In addition, when recording begins, if the person being recorded withdraws their consent, the receiving agent must be able to stop a previously initiated recording and ensure that the recording is not saved.[142]

IV.2.1.6 Data protection officer

When processing is carried out by a public authority, with the exception of courts or independent judicial authorities, acting in their judicial capacity, or in the private sector. In this case the processing is carried out by a controller whose core activities consist of operations of or processing requiring regular and systematic supervision of data subjects, a person with expert knowledge of data protection legislation and practices shall assist the controller or processor to monitor the accordance with the Regulation.[143]

In comparative terms, Data Protection Officer (DPO) is similar, but not the same as a Compliance Director. The former must also be proficient in IT process management, data security (including dealing with cyber attacks), and other critical business continuity issues in the industry, retention and processing of personal data and confidential data. Also, the required skill set goes beyond

[140] Zarsky, op. cit., 2017, pp. 66-90.
[141] Žák, op. cit., 2017, p. 32.
[142] Carnevale, op. cit., 2018, s/p.
[143] European Commission, 2016.

understanding legal compliance with data protection laws and regulations.[144]

The appointment of a DPO in a large organization will be a challenge for the Council as well as for the individual in question. There are a multitude of governance issues and human factors that organizations and companies will need to address, considering the scope and nature of the designation. In addition, the holder of the position will need to create his own support team and will also be responsible for his own continuous professional development, as it must be independent of the organization that employs them, effectively as a "mini-regulator".[145]

More details on the role and function of the data protection officer were provided on December 13, 2016 (revised April 5, 2017) with a guidance document.[146]

IV.2.1.7 Pseudonymization

The GDPR of the European Union refers to encryption of data as the safest formula for its protection. In fact, it states in articles 33 and 34 that if the information is encrypted, even if a leak occurs, it is not necessary to notify those affected, or the corresponding administrative authority.[147]

Such process leads to the understanding of pseudonymization as something required for any storage of personal data about people in the EU as an alternative to another data anonymization option.[148]

IV.2.1.8 Data breaches

Under the GDPR, the Data Controller shall have a legal obligation to notify the Supervisory Authority without undue delay. Notification of a data breach is not subject to any de minimis rule and shall be notified to the Supervisory Authority within 72 hours of learning of the data breach (Article 33). Persons should be notified if an adverse impact is determined (Article 34). In addition, the data processor must notify the controller without delay after learning of a personal data breach (Article 33).[149]

144 Tantleff, op. cit., 2017, s/p.
145 Goddard, op. cit., 2017, s/p.
146 Tantleff, op. cit., 2017, s/p.
147 Zarsky, op. cit., 2017, pp 80-87.
148 Kennedy, op. cit., 2017, s/p.
149 Žák, op. cit., 2017, pp 90-95,

However, notification to data subjects is not necessary if the controller has implemented appropriate technical and organizational protection measures that make personal data unintelligible to those who are not authorized to access, such as encryption (Article 34).[150]

IV.2.1.9 Sanctions

The following sanctions may be imposed:

a) Written notice in cases of prior and intentional default,
b) Periodic data protection audits.

A fine of up to 10,000,000 or up to 2% of the previous year's worldwide annual turnover in the case of a company, whichever is greater, when there is a violation of the following provisions (Article 83, paragraph 4):

a) the obligations of the controller and the processor in accordance with Articles 8, 11, 25 to 39, 42 and 43;
b) the obligations of the certifying body in accordance with Articles 42 and 43;
c) the obligations of the supervisory body in accordance with Article 41.[151]

A fine of up to 20,000,000 or up to 4% of the annual turnover of the previous year, in the case of a company, whichever is greater, when the following provisions are violated:

a) The basic principles of processing, including the conditions for consent in accordance with Articles 5, 6, 7 and 9, the rights of data subjects pursuant to Articles 12 to 22;
b) Transfers of personal data to recipients of third countries or international organizations in accordance with Articles 44 to 49;
c) Any obligation, pursuant to the law of the Member States, adopted pursuant to Chapter IX;
d) Failure to comply with a temporary or definitive order or limitation of the processing or suspension of data flows by the supervisory authority pursuant to Article 58 or lack of access in: breach of Article 58).[152]

[150] Carnevale, op. cit., 2018, s/p.
[151] Sobolewski, Mazur, & Paliński, op. cit., 2017, s/p.
[152] Zarsky, op. cit., 2017, pp. 50-55.

IV.3 Privacy Shield

The Privacy Shield decision adopted on 12 July 2016 made its structure operational on 1 August 2016, protecting the fundamental rights of anyone in the EU whose personal data is transferred to certified companies in the United States for commercial purposes and brings legal clarity to companies that rely on transatlantic data transfers.[153]

Moreover, the European Commission has undertaken to review the agreement annually to assess whether it continues to ensure an adequate level of protection of personal data. The first and second annual review took place in September 2017 and October 2018, respectively.[154]

Regarding US government actions, on September 12, 2019, Director-General for Justice, Consumers and Gender Equality Tiina Astola and U.S. Secretary of Commerce Wilbur Ross launched discussions for the third EU-US review. Privacy Shield (statement). The findings of this report are based on meetings with representatives of all U.S. government departments tasked with administering the Privacy Shield, including the Department of Commerce, the Federal Trade Commission, the Office of the Director of National Intelligence, and the Department of Justice, which took place in Washington in September 2019, as well as contributions from a wide range of stakeholders, including feedback from companies and privacy NGOs. Representatives of the EU's independent data protection authorities also participated in the review. Notwithstanding, there are still pending disputes before the Court of Justice of the European Union in the USA. transfers, which may also affect the Privacy Shield. A hearing was held in July 2019 in Case C-311/18 (Schrems II) and, once the Court's judgment has been issued, the Commission will assess its consequences for the Privacy Shield.[155]

Unfortunately, the Privacy Shield is no longer in place. This is because the European Commission[156] has made many requirements for the US in order to adapt it to the GDPR, which have not be complied so far. Then, that contract is suspended, at least for now.

Yet, the U.S. is still working on the initiative. Sen. Kirsten Gillibrand[157] (D-NY) recently published an initial 41-page "discussion outline" of the proposed legislation, the 2020 Data Protection Act, which she formally introduced as S-3300, which if approved, would create a federal data protection agency.

---

153 European Commission. (October 18, 2017a). EU-U.S. *Privacy Shield*: First review shows it works but implementation can beimproved. Brussels: European Commission - Press release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3966

154 European Comission, 2018.

155 European Commission. (October 23, 2019). *EU-US Privacy Shield*: Third review welcomes progress in identifying steps for improvement. Brussels. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134

156 European Commission.

157 Gillibrand, Kirsten (February 13, 2020). S.3300 - Data Protection Act 2020. In: 116th Congress, 2D Session, (2019-2020). *S.3300*: To establish a Federal data protection agency, and for other purposes. In the Senate of the United States. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/3300/text

Among other things, this new federal department would have the authority to oversee and regulate the profile of large-scale individuals and the processing of biometric data to uniquely identify an individual.

Senator Kirsten Gillibrand[158] said that "illegality in the data privacy space can give rise to new and unexpected forms of injustice" [159] and further emphasized that "the United States must strive to take the lead and do something about data protection".[160]

In addition, the same politician[161] said that the Data Protection Act would "deal with it head-on" by "establishing [an] independent federal agency and would serve as an 'arbitrator' to define, arbitrate and enforce rules to defend the protection of our personal data interests."

Caitriona Fitzgerald, currently policy director of the Electronic Privacy Information Center (EPIC), comments that: "Senator Gillibrand has put forward a bold and ambitious proposal to protect americans' privacy. The U.S. faces a privacy crisis. Our personal data is under attack. Congress should establish a data protection agency".[162]

Mary Stone Ross, associate director of EPIC and former president of California's consumer privacy, also opines in the same sense as her companion: "'Companies' inconsistent approach to complying with the California Consumer Protection Act proves that enforcing privacy regulations is critical. Fortunately, the Data Protection Act".[163]

The Data Protection Agency[164] would have three main missions:

a) First, it would provide Americans with control and protection over their own data by applying data protection rules.
b) The agency would enforce statutes and privacy rules around data protection, as authorized by Congress or themselves. It would use a wide range of tools to do this, including civil sanctions, precautionary measures and equitable remedies.
c) The agency would also receive complaints, conduct investigations and inform the public about data protection issues.

Gillibrand[165] explained that "if it looks like a company is doing bad things with its data, the Data Protection Agency would have the authority to launch an investigation and share findings." The senator also explained that the new agency would work to maintain the world's most innovative and successful

[158] Gillibrand, id.
[159] "ilegalidade no espaço de privacidade de dados pode dar origem a novas e inesperadas formas de injustiça" (Gillibrand, 2020, s/p, tradução nossa)
[160] "os Estados Unidos devem se esforçar para assumir a liderança e fazer algo em relação à proteção de dados". (Gillibrand, 2020, s/p, tradução nossa)
[161] Gillibrand, id.
[162] Kimery,A. (Feb 27, 2020). *Senator proposes new digital privacy agency with sweeping powers.* Categories: Biometrics News, Government Services. Available at: https://www.biometricupdate.com/202002/senator-proposes-new-digital-privacy-agency-with-sweeping-powers
[163] Kimery,id.
[164] Gillibrand, op. cit., 2020, s/p.
[165] Gillibrand, id.

technology sector and ensure fair competition in the digital market, promoting data protection and privacy innovation in all sectors; develop and provide features such as Privacy Enhancing Technologies (PETs) that minimize or even eliminate the collection of personal data; and would ensure equal access to privacy protection and protection against "pay for privacy" or "take or drop" provisions in service agreements, "because privacy, including online privacy, is a right that must be enforced".[166]

In this way, the Data Protection Agency

> would prepare the U.S. government for the digital age by advising Congress on emerging privacy and technology issues such as deepfakes and encryption. It would also represent the United States in international data privacy forums and report future data treaty agreements.[167]

According to the senator[168], the United States is behind of some countries in this sense and also points out that most other developed economies in the world already have an independent agency that is responsible for acting in the face of the challenges of data production, as well as other factors of the digital world.

Gillibrand[169] called the segmentation of personal data a "national crisis" and compared the creation of a new agency in response to the creation of the Department of Homeland Security after the September 11, 2001 attacks.

Gillibrand[170] wrote on his Medium page, but

> Children from all over the country often use platforms like YouTube, Instagram and Tik Tok. These companies can monitor their activities, see what types of content they choose to watch, and which pages they choose to visit. But we don't know what these companies are doing with this information. Can they share my teen son Theo's data from their Instagram page with advertisers? What are the limits on how and why they collect your information? What if Henry decided to download a new app for his phone, or worse, for my phone, would that app company have backdoor access to all the phone data?

Gillibrand[171] provided examples of a fitness app that monitors the heart rates of users who sell data to a health insurance company or a technology company that determines credit scores and displays ads to predatory lenders.

Concerning legal consequences of the political assumptions above, Pierce and Frank[172] described what the senator observed:

> In opposition to the Online Privacy Act, a bill introduced by Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA) that would also create a new privacy agency, Senator Gillibrand's bill would not create a new federal privacy comprehensive law. Instead, it focuses on creating the Data Protection Agency and its rule-making authority. However, several aspects of the

---

166 Kimery, op. cit., 2020, s/p.
167 Gillibrand, op. cit., 2020, s/p.
168 Gillibrand, id.
169 Gillibrand, id
170 Gillibrand, id.
171 Gillibrand, id.
172 Pierce, J. &, Broomell, F. (February 19, 2020). *Sen. Kirsten Gillibrand Proposes New Digital Privacy Agency.* Posted in Congress, Data Privacy, Federal Trade Commission. Available at: https://www.insideprivacy.com/united-states/congress/sen-kirsten-gillibrand-proposes-new-digital-privacy-agency/

> new agency's authority provide valuable information about the appearance of privacy regulation at the federal level under the law.

Pierce is an expert in privacy, cybersecurity and consumer protection issues, including privacy and cybersecurity compliance obligations, preparation and response to cybersecurity incidents, and defense against regulatory investigations and class action litigation. His firm, Pierce & Broomell[173], is specialized in data privacy and cybersecurity practices and litigation and served as a Marine Corps intelligence officer. In a comparative perspective, they also highlight:

> For example, one of the most notable aspects of the proposed agency is involvement in the supervision of 'high-risk data practices'. 'High-risk data practices' include 'systematic or extensive assessments of personal data that are based on automated processing... on which decisions that have legal effects on [an] individual or household are based;' 'any processing of biometric data for the purpose of identifying only an individual;' e' 'processing the personal data of an individual who has not been obtained directly from the individual'.
> It also includes 'sensitive data uses', [...] defined to include 'the processing of data in a manner that reveals' personal data such as [...] race, religion, sexuality, or familial status, [...] of an individual. [...] definition of 'personal data' is very similar to the definition of 'personal information' under the California Consumer Privacy Act ('CCPA'), with a few key divergences (for example, Senator Gillibrand's definition applies to particular individuals or devices, but not to households).[174]

Gillibrand's[175] proposed a law defining high-risk data practice by a covered entity as activities involving the following practices:

a) A systematic or extensive assessment of personal data that is based on automated processing, including profiling, and on which decisions that produce legal effects on the individual or family or that significantly affect the individual or family are based;
b) use of sensitive data;
c) Systemic monitoring of large-scale publicly accessible data; processing involving the use of new technologies, or combinations of technologies, which creates adverse consequences or potential adverse consequences for an individual or society;
d) Decisions about an individual's access to a product, service, opportunity or benefit that is based on any extension in automated processing;
e) Any large-scale profile of individuals;
f) Any processing of biometric data with the objective of identifying exclusively an individual;
g) Any processing of genetic data, which is not processed by a healthcare professional, to provide medical assistance to the individual;

[173] Pierce, & Broomell, id.
[174] Pierce, & Broomell, id.
[175] Gillibrand, op. cit., 2020, s/p.

h) Combine, compare or compare personal data obtained from multiple sources;

i) Process the personal data of an individual that was not obtained directly from the individual;

j) Processing that involves tracking an individual's geolocation; And

k) The use of personal data of children or other vulnerable individuals for marketing, profiling or automated processing purposes.

In their analysis, Pierce & Broomell[176] said that the new agency would be in charge of

> ensure that privacy practices are 'fair, fair, and comply with fair information practices' and develop privacy and data protection model standards and guidelines; oversee 'very large' covered entities, including requiring periodic reports and conducting examinations to assess compliance with federal privacy law; and prohibit 'unfair or misleading acts or practices' for all covered entities. The bill grants the agency's regulatory authority the identification of practices that would be considered 'unfair' or 'misleading'.

In addition, the Data Protection Agency:[177]

> would have the authority to coordinate with the appropriate federal regulatory agencies in order to establish procedures to provide timely responses to consumer complaints regarding the covered entities. Similarly, the agency would have significant enforcement authorities, including the ability to conduct joint investigations with the subpoena authority, seek equitable and legal solutions, terminate or reform contracts, and enforce civil penalties.

As consequence, Gillibrand's[178] proposal would allow state attorneys general to bring civil lawsuits in their state to enforce the rules of the bill or its agency and only prevent state privacy laws that are inconsistent with federal laws.

Considering the regulation in force, in the US the Federal Trade Commission[179] (FTC) is the authority responsible, among other things, for enforcing antitrust laws and reviewing proposed mergers. The FTC also contains the Bureau of Consumer Protection, which allows you to address competition and privacy issues. Last year, both the FTC and the Government Accountability Office appealed to Congress for a federal privacy law. Nevertheless, on January 1, 2020, the California Consumer Privacy Act went into effect, which grants California residents new rights to know what personal information companies hold, to access and delete that information, and to opt out of making a company sale of their personal information.[180]

The issue of Nielsen Holdings N.V. and Arbitron Inc. demonstrates the FTC's ability to identify

---

176 Pierce, & Broomell, op. cit., 2020, s/p.

177 Pierce, & Broomell, id.

178 Gillibrand, op. cit., 2020, s/p.

179 Federal Trade Commission. Protecting America's Consumers. (October 2019). *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority.* Available at: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

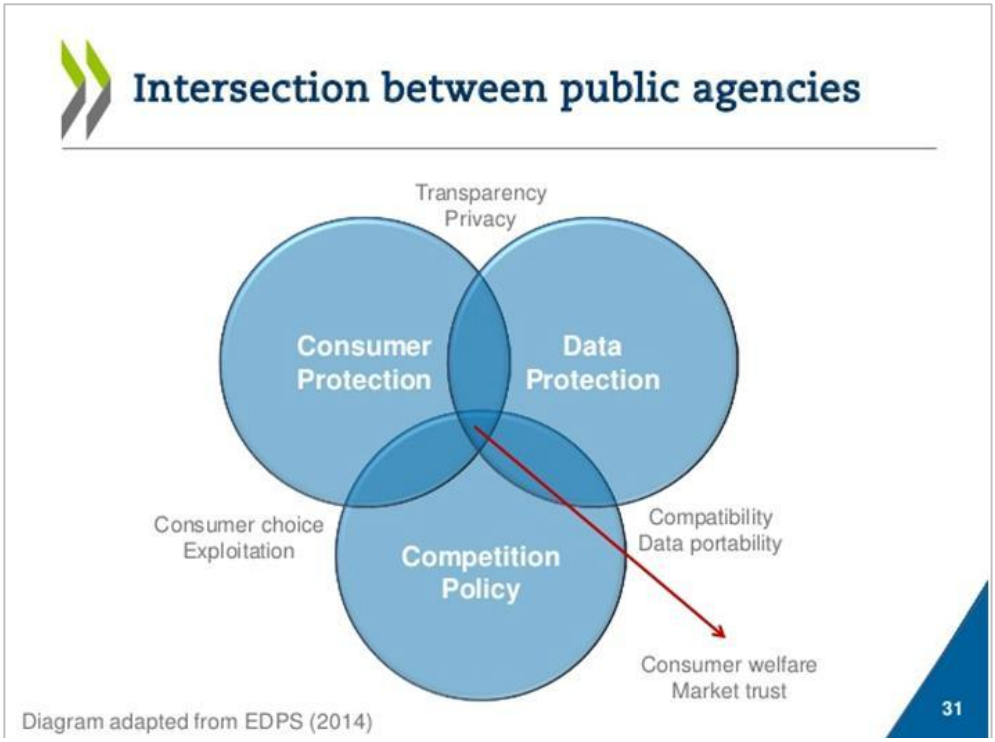
180 Paul, K. (Dec 30, 2019. *California's groundbreaking privacy law takes effect in January. What does it do*? Available at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do

the importance of data in M&A analysis. As a backdrop, Nielsen and Arbitron competed in providing syndicated audience-platform measurement services to media companies and advertisers.[181] According to Mitretodis & Euper[182], the FTC found that access to data represented a significant barrier to entry and obtained a consent order requiring the disposal of assets for Arbitron's multi-platform audience measurement services business, which also included including audience-level demographic information and related technology and intellectual property.

IV.4 Confrontation Between Data Protection Laws and Competition

The Organisation for Economic Co-operation and Development (OECD) has been discussing the intersection of these fields since 2016, as shown in Figure 6:

Figure 1 - Intersection Between public agencies



Source: Thlemann, A. & Gonzaga[183]

[181] Mitretodis, A., & Euper, B. (March 9, 2020). *Interaction Between Privacy and Competition Law in a Digital Economy Part-2*. Published by Fasken Martineau DuMoulin LLP. Available at: https://www.competitionchronicle.com/2020/03/interaction-between-privacy-and-competition-law-in-a-digital-economy-part-2/

[182] Mitretodis, & Euper, id.

[183] Thlemann, A., & Gonzaga, P. (November 2016). *Big data:* Bringing competition policy to the digital era – OECD Competition Division - November 2016 OECD discussion. p. 31. Available at: https://www.slideshare.net/OECD-DAF/big-data-bringing-competition-policy-to-the-digital-era-oecd-competition-division-november-2016-oecd-discussion

Concerning the OECD chart, in recital 9 of the GRPD, there is a forecast of a:

> [...] fragmentation in the implementation of data protection across the Union, legal uncertainty [...] Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may impede the free flow of personal data throughout the Union.[184]

Ahead, the text also states that such differences can also provide a distortion of competition.[185] In such sense, GDPR considers that differences between the legal structure from one state to another cause distortions in competition, in other words, can lead to unfair competition.

On the other hand, this diferentiation also leaves room to form a defense thesis that the startup that eventually processes data unfairly did so in a guilty manner. This is caused by following its own local laws. Thereby, it is clear that such a thesis would be considered only here in cases where the country was not a member of the European Union and had no international treaty , as the privacy shield mentioned above (between US and EU).

Therefore, it is still necessary to think about the question of the application, not only of the European Union, but also of a comprehensive solution (outside the EU). About this concerning Abreu[186] states that, although nowadays, electronic government is increasingly perceived as an instrument of governance that increases transparency, participation, service delivery and the creation and application of the law, there seems to be a need to actually show its results and, specifically, its gains to national administrations. The key is to make them understand that they are European public administrations when they apply EU law and that the decisions they take will be observed and respected across borders.

One thing that is quickly learned when you contact a venture capital firm is that investments consist of finding gaps or competitive advantages. Simply because the pits increase a company's bargaining power with its suppliers and customers, helping the company raise prices, reduce costs and generate higher profits.

The network effect on markets is a great example of a gap. Looking at Airbnb, for example, the more places there are to rent, the greater the demand for the platform, attracting more owners to rent their seats.

This mechanism generates a winning dynamic takes it all. Often, the biggest participant in a market with this dynamic becomes much larger than its competitors. That is the intrinsic characteristic

---

184 EU - General Data Protection Regulation. (2016a). *Recital 9 EU GDPR*. Available at: https://www.privacy-regulation.eu/en/r9.htm

185 EU - General Data Protection Regulation, id.

186 Abreu, J. C. (2018). *Interoperability solutions in the digital single market*. European electronic justice rethought under the paradigm of electronic government.

that attracts investors, if someone is lucky enough to pick the market winner, there is a considerable chance of getting high returns.

Furthermore, the relevant aspect here is that AI brings a new kind of network effect that some call the "data network effect". Machine learning algorithms need data to work. Although the relationship is not linear (more on this later), the prediction/classification of an algorithm increases in accuracy as they ingest more data.

Then, as a company adds more customers, it gets more data to train and refine its algorithms. With more data, the accuracy and overall quality of the product increases. With a better product, customers are more willing to buy and contribute their data. This mechanism helps AI companies follow the customer's adoption lifecycle.

Another self-reinforcing feedback cycle is the "talent attraction cycle". The more data the company has, the more attractive it is for a data scientist to work for them. This means that the team has a greater chance of attracting great talent.

The problem is that a startup initially has no data (or very little) and depends only on a small number of talented individuals. Just as it takes time and resources to network a market, the booster cycle at stake for AI companies requires initial data.

Thus, the holders are the owners of this data. That is the reason why several industry observers have declared that incumbents have an unfair advantage in tackling the AI wave. The good news for AI investors is that it has complexes features. However, simple equation that can explain part of the success of AI companies can be:

Success = data + machine learning[187] talent (ML)**+ algorithms**

In plain English, the formula demonstrate that successful and defensible AI companies will have sufficiently large datasets that ML employees can use to create the best algorithms.

A useful method for thinking about the advantage in AI is to observe the 2×2[188] matrix. The matrix plots the amount of data available per use case on one axis and the nature of the companies currently addressing each of them (technical versus non-technical) on the other.

The next step is to analyze the results in terms of starters versus startups. Large technology companies with a large amount of data. Taking account the use cases addressed by large technology companies where each potential customer has large amounts of data, the existing advantage is

[187] Machine Learning, is one of several Implementations of Solutions as far as artificial intelligence.
[188] Determining mathematical matrix.

considerable consistent. In addition to the typical advantages of the holder, large technology companies also have stacks of data that have accumulated for years.

Large companies also benefit from the brand and greater financial resources to offer the best machine learning talent, which will develop the best algorithms. Thus, it is clear that new startups should not go head-to-head with those responsible for technology in this situation. Instead, startups should follow Google from the beginning.

Non-technical companies may also have to deal with large quantities of data, yet the existing advantage is not only strong in this part of the matrix. Indeed data can matter even more than the algorithms themselves, especially since deep learning emerged. Therefore, even in this case, these companies will have comparative advantages in economic terms.

In addition, large technology companies are continually opening new ML packages, transforming algorithms into commodities, especially for object recognition, language or speech models (generalized ML). Nevertheless, non-technical companies sitting on large data sets can get relevant results using generously pre-trained open source packages in technology companies' datasets.

Therefore, even a large, non-tech company can have a high level of machine learning knowledge and create better AI products in a small startup with better ML experts because it has access to more data. As a consequence, one should probably weigh data above ML talent in the equation: Success = data * data + ML talent + algorithms.

In case of large technology companies without too much data, they are a good example in predicting the probability of a lead undertaking becoming a customer (lead score). However, it is important to note that each lead does not have enough data to create a sufficiently good prediction using generalized ML even if While they have hundreds of data points and many predictors in Customer Relationship Management (CRM) or the marketing automation tools.

Therefore, those large companies will need to purchase a product built on a larger dataset. The question here is whom would be the right player to sell this product. In a deeper analysis, the economic advantage here is less clear. Even so, there can still be many opportunities for startups, especially if they can:

a) Combine different data sources that large technology companies don't[189] have (for example, Salesforce doesn't have access to Hubspot data); or

b) Generate additional proprietary data.[190]

[189] Salesforce is a company based in the United States, votlada for software, which produced the CRM known as Sake Cloud.

[190] Coppey, L. (Oct 17, 2017). *Routes to Defensibility for your Startup AI*: A simple framework for understanding the impact of data network effects and incumbents' advantages in your industry. Available at: https://machinelearnings.co/routes-to-defensibility-for-your-ai-startup-2875a1b51d4e

Going further, some segments of agriculture and health are good examples of where no large technology company dominates the market and where each customer has only a small amount of data.

The positive aspect of the new equation (success = data * data + ML talent + algorithms) is that when data is initially available in smaller quantities, its impact is more limited and talent and ML algorithms, having a greater impact on output. Thus, incumbents have fewer unfair advantages, as a startup with the right talent in ML and innovative algorithms has a chance to thrive in a market mainly where data is scarce.

Thinking of a Software as a Service (SaaS)[191], solution for greenhouses can combine data from multiple greenhouses and get the best yield forecast. Not every greenhouse owner probably is relying on data sets big enough, but they would benefit considerably from an AI agent building a better forecast or even controlling the entire greenhouse.

Venture capitalist Tom Tunguz has an interesting counterpoint in the current matter, by applying some lessons from the world of Adtech. Another reason why large data sets are not available is that they are stored in silos not only from between different clients, but also between different SaaS tools. Some of these tools are engagement systems (a website) and others are records systems (a marketing automation tool). An AI startup that can stand between these two data sets may well be in the best position to become what Chen[192] calls the "intelligence system."

When analyzing the CRM use case again, there is the question whether the paths of the reagents do not react to marketing guarantees as good predictors of their probability of purchase. The problem is that Salesforce does not have this data because it is locked in the Hubspot database.

Similarly, Hubspot does not know how fast leads are evolving in the sales pipeline. Therefore, as long as data is scarce in this market (left side of the matrix), neither Salesforce nor Hubspot is in the right position to create the best prediction. An AI startup that builds its forecasts across both databases, on the other hand, can outperform Salesforce and Hubspot in this venture.

A good way to think about this matter is to visualize datasets as complementary assets in the value chain. Seemingly harmless new AI startups can partner with companies that incumbents never want to partner with and thus create complementary assets to protect them. The counter to this statement is that any company that relies on a single non-proprietary data source is much less defensible than one that combines several.

---

[191] It is a Software to serve them, and can be used through an internet network, it is aimed at distribution and marketing of software.

[192] Chen, J. (Apr 24, 2017). *The New Moats*: Why Systems of Intelligence™ are the Next Defensible Business Model. Available at: https://news.greylock.com/the-new-moats-53f61aeac2d9

Resuming, answering the question about whom makes money from the data, whether it is the company that is generating the data, or company is storing it or even the company is building the best ML product on top of them.

This is nothing new in AI startups, but it can have an opposite dimension as people realize the value of their data. Just as Twitter has dispached all companies developing alternative Twitter customers, Salesforce can overcome any startup that extracts a lot of value from the data stored on its platform.

If a company cannot collect data from multiple customers or from multiple SaaS tools, or even if it is simply not enough to create a good enough forecast, the company can try to generate additional data from its own SaaS offering. This is a unique opportunity to create a proprietary dataset that no other holder has.

This reasoning can be summarized by drawing learning curves that describe how much time, effort, or funding is required to achieve high enough forecast accuracy to meet customer expectations.

With little time, effort and financing, the company can get enough data to meet customer expectations. Therefore, defensibility is relatively limited. This applies primarily to cases where the data used is available to the public.

At the opposite end of the spectrum, in a situation where data is scarce and requires a lot of time, effort and funding, the curve would probably look like this:

a) In such a situation, it takes a lot of time, effort and funding to achieve sufficiently high accuracy. Therefore, defensibility is strong.
b) It is important to emphasize that these situations are very theoretical and are here only to provide a framework for thinking about the defensibility of the effect of the data network.

The second situation in which data is scarce can create a lot of defensibility, but it can also put the startup in a difficult situation, because the company needs to wait until the A series to meet customer expectations.[193]

ML defensibility and SaaS are also not mutually exclusive. A very long product roadmap[194] and a superior UX or blocking of user data still contribute greatly to a company's defensibility.

Protecting people's privacy is often confronted with innovation and economic interests. This concern is not entirely unfounded. As businesses face growing trust shortfalls, small businesses and startups fear that privacy laws will fall disproportionately on them. However, this need not be the case:

[193] Coppey, op. cit., 2017, s/p.
[194] Refers to the user experience developer.

strong privacy laws can establish clearer ground rules that level the playing field for businesses large and small and protect individuals from unfair, surprising, and privacy-invading practices.

Last year, there was an ongoing debate about whether the EU General Data Protection Regulation (GDPR) is this clear and strong privacy framework. Some have argued that the GDPR may well stimulate innovation, but several companies have hit the headlines blaming the GDPR for closing their businesses in the EU.

The Center for Democacy & Technology (CDT) testified in 2019 on this matter before the Senate Judiciary Committee. The message was that the evidence that the GDPR itself harmed small and medium-sized enterprises is anecdotal and ultimately inconclusive. Many companies, large and small, have used the GDPR as an opportunity to improve their data manipulation practices and invest in privacy. [195]

For example, the French Information and Freedoms Commission (CNIL) in 2018[196] issued a warning against small advertising technology company Vectuary for failing to obtain appropriate consent to obtain geolocation data from scripts embedded in its partners' mobile applications. While some have argued that this could be the end of online advertising, the investigation was recently dropped after the company made changes to its disclosures. CNIL has also worked with several other location analysis companies. As the CNIL explained, data protection regulators are not interested in "ending the existence of companies if there is another alternative" and "will be kinder and will have time to first explain to companies how they should do things".[197]

While some minor violations of the GDPR by small businesses located outside the European Union can be forgiven (especially early in law enforcement), U.S. companies that are knowingly and actively collecting data to do business in the EU ignore the law on their own.

To continue operating in the EU, entities located outside the EU that fall within the extraterritorial scope of the law, as well as the requirements of the Data Protection Officer, are required to appoint a representative with commercial residence or staff in the EU as a contact person for all. Such requirement causes problems with data protection, although this can be accomplished through a virtual DPO.

Otherwise, its ability to operate in the EU may be limited and the EU may even impose fines issued against US companies. In recent years, there has been increased cooperation between

---

[195] Jerome, J. (April 1, 2019) *The GDPR's Impact on Innovation Should Not Be Overstated*. Center for Democacy & Technology (CDT). European Policy, Privacy & Data. Available at: https://cdt.org/insights/the-gdprs-impact-on-innovation-should-not-be-overstated/

[196] National Commission on Information Technology and Freedoms. (2018). *Mobile apps*: formal notices for failure to consent to the processing of geolocation data for advertising targeting purposes. Available at: https://www.cnil.fr/fr/applications-mobiles-mise-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire-2

[197] National Commission on Information Technology and Freedoms, id.

regulators and regulators in the United States and the European Union. As the US has EU assistance enforcing its laws abroad, it is premature to think that the EU will not be able to impose fines on companies located in the United States.

The first view of the approach DPA can take in the GDPR in cases of US companies, which left the UK in November 2018. The UK ICO issued a warning to the Washington Post about how it was obtaining consent for cookies. The ICO concluded that consent was not given freely under Article 7 of the GDPR[198] because the document did not offer a free alternative to the acceptance of cookies. However, the ICO noted that there was little it could do if the Washington Post decided not to change its practices. This ICO commentary leaves its ability and likelihood to cast doubt on enforcement actions.[199]

However, it is too early to draw inferences based on this note. It is noteworthy that the first company to be fined by the GDPR by the ICO was a Canadian company. Other DPAs may also decide not to respect the decision. Indeed, the EDPB issued a clarification document on the obligations to the GDPR of companies not located in the EU. Therefore, this debate on the scope of obligations is likely to continue.

As others have pointed out - the GDPR alone does not provide the powers to block websites. The reason why is that the GDPR is not about websites, it is about data (which includes some sites, but many other things besides that).

The first application option within the GDPR is by imposing fines. In terms of EU policies, it has being the favorable approach. If the offender has absolutely no presence in the EU, it may be difficult to collect those fines, but for any of the large multinationals actually affected by the GDPR - fines are a good enforcement mechanism. Nevertheless, there will be companies that will decide not to manipulate any EU data to try to avoid the applicability of the GDPR, but this is likely to lead to unfavorable results.

Aside from the financial penalty, there is a second execution option that is in progress. The EU has a regulation in place that faces challenges by dealing economic actors operating primarily or exclusively in the digital space. EU authorities (usually at national and non-EU level) take action to apply regulation in new and unusual ways in the digital space, for instance by blocking a website. It Is Possible, but there are other enforcement options and they can be very subtle (and effective), for example, providing users with an ISP-generated warning every time they visit a specific website or access some online service. Website blocking actually happens now in the EU, although it only refers to sites that have proven to have a criminal offence behind them.

---

[198] Hunton Andrews Kurth. (November 21, 2018). *UK ICO Issues Warning to Washington Post Over Cookie Consent Practices*. Privacy & Information Security Law Blog, Posted in Enforcement, European Union, International. Available at: https://www.huntonprivacyblog.com/2018/11/21/uk-ico-issues-warning-washington-post-cookie-consent-practices/

[199] Hunton Andrews Kurth, id.

Finally, there is the fact that the GDPR will have a large impact not only on companies that use data, but also it is becoming a tool to inform people about where and how their data is being used. This perspective will change the usage profile of online services (I know it has already changed mine), which will result in changes in the way websites collect information. Before, there used to have no cost associated with collecting information, now there is more likely to exist one.

Ironically, instead of Europe blocking websites, websites are blocking Europe. Some good examples are sites that use the "GDPR Shield" service to block European visitors, preventing from deleting from GDPR. Major US news sites are still blocking Europeans due to the GDPR.

There is doubt regarding the possibility of EU effectively blocks sites when they do not comply with the GDPR. In practical terms, the answer is negative, as the GDPR involves processors and controllers but their interest lies in the context of evidence.[200]

That said, millions of companies have the power and legal authority to block access to the site by their employees. The EU shares this capacity, but only as an employer of around 35,000 employees (more than 15,000 non-employed workers).

Considering the EU an international body, it has a role in the application of the GDPR, but not against controllers or their websites, only against nations and international bodies. Like most soft energy projections, these spanking is usually done very quietly, as when it rolled in the U.S. in December 2017 (to be fair, since 2017, the U.S. has become an easy target for everyone, which in terms of future stability is very unfortunate).[201] Yet, this application is carried out only in the context of the unfortunate decisions of the country involved, while in cases of the law or the unfortunate legislation (see recital 115 and Article 48 of the declaratory, successfully deployed even before the GDPR is applicable) and not on government websites or other web sites.[202]

Instead, the GDPR is applied by 48 independent but cooperating supervisory authorities (28 national regulators, 18 provincial regulators, the EDPS with a roving document and the EDPB that creates cats and guides the courts), courts of Member States, courts laws around the world applying local contracts that import aspects of the GDPR, and courts around the world executing enforcement orders of the courts of the member states in accordance with the usual rules of private international law (that is, business as always).[203]

---

[200] Daigle, B., & Khan, M. (September 2019). *One Year In*: GDPR Fines and Investigations against U.S.-Based Firms. U.S. International Trade Commission (USITC) Executive Briefings on Trade. Available at: https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf

[201] Cabral, F. F. (Maio 19, 2018). *O impacto da legislação europeia para brasileiros com negócios na internet*. Brasil: ConJur. s/p.

[202] Roncolato, M. (Maio 28, 2018). *Nova lei de proteção de dados da Europa*. E o efeito no Brasil. Brasil: Nexo. s/p.

[203] Cabral, op. cit., 2018, s/p.

None of the regulation above is ordered by the EU. Even the Supervisory Authorities are by law (consequences of schrems' 2015 Safe Harbor case) not bound by conflicting EU laws or the GDPR or EU Member States or their conflicting laws. For instance, the UK Information Commissioner has legislative powers similar to those of Cabinet Ministers, but unlike Cabinet Ministers, it has independent government fundraising powers).[204] For the same reason, since 2015, the EU has lost the power to make legally binding trade agreements in relation to personal data flows. United Kingdom (cf. Brexit) and the USA (cf. "Privacy Shield") make unilateral decisions.[205]

Yet, there are less certainty in case of American companies with no physical presence in the EU. The GDPR addresses this issue by requiring companies without an establishment in the EU to have a representative located there.[206] The result depends on the judgment of the EU member state. Some EU countries, such as Germany, take a stricter approach to data privacy and may not be as lenient.

Finally yet importantly, EU regulators rely on international law to issue fines. A clause is written in the GDPR itself stating that any action against a company outside the EU must be filed in accordance with international law. However, this is not effective if it is a small startup and is causing unfair competition with another EU startup the startup itself needs to be able to start a low-cost action. In any case, the EU needs to protect them and push them back - with fines and even allowing the ISP to be blocked, whereas startups can fulfil their national state and request it.

---

[204] Silva, H. S. S. (Janeiro 5, 2017) *A protecção de dados pessoais na era global*: o caso Schrems. Lisboa, 109 fl. Dissertação (Mestrado em Direito, na área de Ciências Jurídicas Forenses) - Faculdade de Direito da Universidade Nova de Lisboa. Available at: https://run.unl.pt/bitstream/10362/20567/1/Silva_2017.pdf

[205] European Union. (2018). Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC. General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[206] Wolford, B. (2020). *GDPR compliance checklist for US companies*. Available at: https://gdpr.eu/compliance-checklist-us-companies/

V. ABUSE OF DOMINANCE OF THE TITANS OF TECHNOLOGY

V.1 Unfair Competition in the Digital Single Market

Is there an abuse of dominance in the digital single market? To answer the question, it is necessary to proceed initially to the historical framework of the concept of data. On the other hand, it is not possible to carry out an analysis of fairness in European jurisprudence without first having carried out a context synchronized with the realities of personal data breach and abuse of dominance at the international level.

There are many conflicting decisions, even within domestic jurisdictions, as in Germany for instance. In a trial of 25.10.2018, the Oberlandesgericht Hamburg concluded that violations of the GDPR are primarily actionable by competitors. However, this decision only applies if the additional purpose of the violated GDPR rule is also to protect market behavior.[207]

With its decision, the Court asserts the competitor's right of action in accordance with German unfair competition law in relation to the Data Protection Directive, as well as in relation to the GDPR. The Court states that the data protection directive obviously does not contain a comprehensive sanctioning system prohibiting actions against data protection breaches in accordance with civil law. While the Data Protection Directive is intended to fully harmonize data protection law in the European Union, the GDPR Directive does not contain a comprehensive system of remedies.

In such sense, the Court ruled that the GDPR, such as the Data Protection Directive, does not contain a comprehensive sanctioning system which excludes competitors' actions in accordance with competition law.

Furthermore, in the Court's view, the provisions of the GDPR do not limit civil actions against violations of the GDPR to data subjects whose personal data have been processed by the controller. According to the judges, the GDPR defines only a minimum level of resources and is open to other resources and sanctions that are not explicitly regulated within the GDPR. Adding, the Landgericht Würzburg (District Court, Würzburg) reached the same conclusion in its court decision of 13.09.2018.[208]

In another case, as of 08.08.2018, the Landgericht Bochummaintained held a different view. There, the Court considered that the provisions of Art. 77 to 84 of the GDPR should be seen as an

---

[207] Eckhardt, J. & Steffen, N. (January 16, 2019). *Is a violation of a GDPR rule at the same time a violation of competition law*? International Network of Privacy Law Professionals (INPLP). Available at: https://inplp.com/latest-news/article/is-a-violation-of-a-gdpr-rule-at-the-same-time-a-violation-of-competition-law/

[208] Eckhardt, & Steffen, id.

exhaustive rule which conclusively determines the authorized categories of potential applicants. Therefore, actions beyond these provisions by a competitor are not possible, because with the provisions of the GDPR the European legislature has expressed its intention not to extend the categories of possible applicants.[209]

The Landgericht Wiesbaden (District Court, Wiesbaden) reaches the same conclusion, adding in its decision of 11.05.2018 that, due to the exhaustive provisions of Art. 77 to 84 of the GDPR, there is no gap in legal protection which needs to be fulfilled by competition law.[210]

For academic purposes, it is necessary to highlight that the additional objective of the GDPR rule should be to protect market behavior. The Oberlandesgericht Hamburg also ruled that breaches of the GDPR do not necessarily result in precautionary measures in accordance with competition law.[211]

Some doubts remain in this inquiry:

a) What do other competition authorities (when they exist) think about it?
b) Will these authorities cooperate with each other? How's that going to work?
c) What is the application of this?
d) The Commission's response, on the one hand, was lukewarm. Can Facebook's decision in Germany serve as a model for EU action? Even if you are "in the area between competition law and privacy" and are based in part on German law?

What does Germany's decision mean for Facebook's plans to integrate Facebook, WhatsApp and Instagram? Under a recently announced plan, the company will unify the underlying technical infrastructure of the various applications, which will make cross-platform communication possible. Although BKA's decision is geographically limited to Germany, it at least presents an additional technical challenge to an already ambitious plan. But only startups and companies in Germany are protected from abusive and unfair competition from Facebook. How can this be extended to the entire European Union and to the whole world?

In the same sense that data privacy spreads around the world, these infringements of competition should also be maintained on all lists of concerns in all countries. It is, in fact, a question left aside. Meaning that all global startups, especially those who want to become unicorns, need to fight for it.

---

209 Hr-On. (May 2018). How GDPR affects recruitment and job adverts. Available at: https://hr-on.com/how-the-general-data-protection-regulation-changes-recruitment-and-job-adverts

210 Eckhardt, & Steffen, op. cit., 2019, s/p.

211 Burgess, M. (March 24, 2020). *What is GDPR? The summary guide to GDPR compliance in the UK.* Wired. Available at: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

The problem is even greater when we talk about the need for international cooperation, since many of the technology giants do not have a single headquarters and their servers are spread across several countries, which makes difficult to establish the competent authority in competition matters.

Only then will you be able to examine the need or not to legislate specific points to ensure the protection of startups, small and medium-sized enterprises, analyzing the decisions of the CJEU, seeking to establish the possible bridges with the design of data protection and competitiveness.

Given that online platforms generate revenue based on behavior prediction and ad targeting, this paper seeks to illustrate when there is domain abuse at this time (Article 102 - Treaty on the functioning of the European Union) From another north, it is argued that the protection of personal data has also emerged as a dimension of competition in terms of quality. With Article 102, consumers can benefit from fair competition, which means: lower prices, quality, choice, improved products and services.[212]

It is expected to determine whether the legislation is sufficient and what needs to be implemented to protect start-ups and small businesses from competing with technology giants, in addition to its effective reach in addressing the different sources of law, its creative/interpretive/integrating function, among other subsidiary issues that are part of an in-depth discussion on this topic.

Technology giants like Facebook have been breaching data since 2004, and this constitutes an abuse of dominant position, unfair competition. The CJEU is deeply wrong, and Germany is absolutely right to extend the GDPR to the concepts of competition law and also to limit Facebook's practices.[213]

The user may not be the only focus on GDPR analysis. The regulation has already advanced, establishing in the recitals the pedagogical way of not imposing fines, of guiding small and medium-sized companies, and including startups. It is paramount that startups can compete fairly, and what Facebook cannot do as it pleases.

As another example, the European Commission has already investigated Google for antitrust concerns regarding the terms and conditions it places on Android-based phone manufacturers.

The European Commission[214] considered that Google offered favorable positioning and displayed its own shopping comparison service on its general search results pages and was fined 2.4 billion euros for anticompetitive conduct. It was also fined 4.34 billion euros by the European Commission in 2018

[212] Official Journal of the European Union, op. cit., 2012, s/p.

[213] Crémer, J., De Montjoye, Y-A., & Schweitzer, H. (2019). *Competition policy for the digital age*. Luxembourg: Publications Office of the European Union. DOI: 10.2763/407537. Available at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

[214] European Comission (2018).

for imposing illegal restrictions on Android device manufacturers and mobile network operators to consolidate its dominant position in general Internet search.

Regarding the dominant position of tech giants, Commissioner Margrethe Vestager, head of competition policy, said that:

> 'Google has used Android as a vehicle to cement the dominance of its search engine,' [...], the EC commissioner in charge of the competition policy, in a press statement. 'These practices have denied rivals the chance to innovate and compete on the merits. They have denied European consumers the benefits of effective competition in the important mobile sphere'. [...].[215, 216]

These cases are under appeal, but illustrate in principle how a platform can use its gatekeeper power in one market to strengthen its position in another.[217]

In other words, the Original Equipment Manufacturer (OEMs) of Google/Android smartphones that was willing to install the Google Play Store should also install Google Search, tying it as domain abuse, excluding other smartphone rivals.[218]

In another antitrust case, the European Commission[219] fined Google 2.42 billion euros for abusing the domain as a search engine, giving the purchasing comparison service itself an illegal advantage.

And it's not just Google, after fining Google billions of euros, the EU is checking how it collects sales information made by competitors on Amazon Marketplace and whether that gives any advantage when selling to customers, led by EU Competition Commissioner Margrethe Vestager.[220]

The question here is about the data that Amazon collects from small merchants on its website. About this matter, Vestager said: "You also use this data to do your own calculations, what's new, what people want, what kind of offers they like to receive, what makes them buy things? This led us to start a preliminary investigation".[221]

The power of the online giants that provide a platform for other companies has drawn fierce criticism from both sides of the Atlantic and prompted the draft EU rules to ensure that platforms

---

215 (McGrath, 2018, s/p., tradução nossa)

216 McGrath, D. (Julho 19, 2018). *Google to Appeal Record EU Fine Over Android*. Available at: https://www.eetimes.com/google-to-appeal-record-eu-fine-over-android/#esso

217 McGrath, id.

218 McGrath, id.

219 European Commission. (June 27, 2017b). *Antitrust*: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service. Brussels: European Commission - Press release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784

220 White, A. (September 19, 2018). *Amazon probed by EU on data collection from rival retailers*. Available at: https://www.bloomberg.com/news/articles/2018-09-19/amazon-probed-by-eu-on-data-collection-from-rival-retailers

221 Bernal N. & Titcomb, J. (July 16, 2019). *EU opens formal competition investigation into Amazon over use of merchant data*. San Francisco: The Elegraph. pp. 10-16.

behave fairly. Whereas last year, Google was ordered to offer equal treatment to smaller search rivals for ads displayed on top of its results.

In a very recent and paradoxical debate, Apple reverted a Commission Decision, regarding "threatening of distort competition".[222]

In a landmark ruling, the General Court of the European Union has annulled the 2016 adoption of a decision taken by the Commission regarding Irish tax rulings granted in favour of Apple. The Court concluded that the Commission failed to prove, to the requisite legal standard, that the tax rulings granted by the Irish tax authorities to Apple constituted State Aid for the purposes of Article 107(1) of the Treaty of the Functioning of the European Union (TFEU).

The Court therefore annulled the Commission's decision on the basis that the Commission did not succeed in showing to the requisite legal standard that there was an advantage for the purposes of Article 107(1) TFEU.[223]

However, there are a lot of missing points in the General Court decision. There is at least one point of view that was just ignored in this annulment. How will startups compete with those aids? The use of data by tech giants is not the only worries for those small business (that sometimes are not even companies yet).

An appeal, limited to points of law only, may be brought before the CJEU against the decision of the General Court within two months and ten days of notification of the decision.

The right way to go in front of this bucket of cold water, is the Commission lodge an appeal to Europe's highest court, in order to keep Commission's zealous campaign against, unfair and distorted competition, low-tax jurisdictions and the international tax planning industry, specially involving technology companies.

Decisions like this, shows that something must to be done in order to make possible this ruling in favour of the Commission without raising questions about the application of Ireland's tax code. The decision came at a sensitive time, when new global rules for taxing digital giants are being debated, and also involving privacy and competition. European Commission should not give up on this fight, the European Union has already defined a set of ethical standards to guide the development of Artificial Intelligence on the continent. Every decision made by an algorithm needs to be verified and explained. Among all technology fields, such as Internet of Things, Artificial Intelligence must be reliable and safe and the companies that created it must be legally responsible for the decisions made by the system. Besides that, a fair competition system that involves not only tax but also privacy and data protection

[222] Commission Decision (EU) 2017/1283 of 30 August 2016 on State Aid SA.38373 (2014/C ex 2014/NN ex 2014/CP).

[223] T-778/16 *Ireland v Commission*, T-892/16 *Apple Sales International and Apple Operations Europe v Commission*. Judgement 15 July 2020.

must be established, without leaving aside the fact that all authorities competence and cooperation should be predicted.

Another dispute that represents a very good step to achieve a global regulation regarding data privacy was the brand new invalidation of Privacy Shield (between EU and USA).[224]

While the disputes are totally different, they both show how the EU is a global player in technology governance and regulation. What joins them is the impact these decisions will have on trans-national business practices and the EU's relationship with multinational companies. Which still needs to evaluate competition and protection to smaller ones (startups).

V.2 Lack of Competition Legislation

When legal privacy and competition settings are analyzed together, three topics deserve greater attention: portability, interoperability, and data merging.

Determining the value of data in cases of concentration is challenging, as is declaring a concentration compatible with the internal market and the EEA Agreement (Case M.8788 - Apple/Shazam).[225]

European authorities have released Apple's acquisition of popular music recognition app Shazam, after months of study on whether the deal would give the iPhone maker an unfair advantage over rival music streaming services like Spotify.

On March 14, 2018, the Commission received notification of a merger that would result in the acquisition of Shazam by Apple, developer and distributor of music recognition applications for smartphones, tablets and personal computers. The notification followed a referral in accordance with a request made on 21 December 2017 by the Austrian competition authority, to whom the acquisition was notified on 12 December 2017; competition authorities from seven more EEA Member States subsequently acceded to the application.[226]

On 23 April 2018, the Commission opened a Phase II investigation due to two distinct non-horizontal and uncoordinated effects:

> (a) the potential foreclosure of competing providers of automatic content recognition ('ACR') software solutions, including music recognition apps, in the territory covered by the EEA Agreement ('the EEA') as a result of conduct such as pre-installing Shazam on iOS or integrating Shazam with iOS or degrading the interoperability of ACR solutions provided by Shazam's competitors on iOS; and

[224] C-311/18, *Facebook Ireland vs Schrems.* Judgement 16/07/2020

[225] European Commission. (September 6, 2018) *Case M.8788 – Apple/Shazam*. Brussels, Article 8(1), Regulation (EC) 139/2004, Commission decision of 6.9.2018. Available at: http://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.pdf

[226] European Commission. *Case M.8788 – Apple/Shazam*. ibid., 2018, p. 7.

(b) the potential foreclosure of competing providers of digital music streaming apps in the EEA as well as in the territories of the Referring States as a result of Apple gaining access to commercially sensitive information on its rivals through the Concentration.[227]

However, having conducted an in-depth investigation into the databases maintained by Apple Music, Apple Music's competitors and Shazam's competitors and examining several possible concerns arising from the merger, the Commission concluded in its decision on 6 September 2018 that the transaction would not significantly impede effective competition on any of the following items:

a) licensing music chart data worldwide, in the EEA or in any of the Referring States;
b) online advertising services in any of the Referring States;
c) digital music streaming applications in the EEA or any of the Referring States; and (iv) ACR software solutions worldwide or in the EEA.[228]

The decision closely examines the digital music industry, including digital music streaming services and ACR software solutions, and the role user data plays in generating insights, product development and targeted advertising. It identifies five distinct relevant markets:

a) Software solution platforms;
b) Digital music distribution services;
c) ACR software solutions, including music recognition applications;
d) Licensing of musical data; And
e) Online advertising.

The Commission left open the possibility of further market segmentation, as there would be no barriers to effective competition in any of the plausible definitions. However, what seems clear in the competitive valuation of these markets is that Apple has a considerable stake (20 to 30%) in software solution platforms and digital streaming applications; while Shazam has a prominent stake (over 30%) in the smart mobile music recognition app market and a more marginal position in the ACR software solutions market (5-10%).[229]

Finally, although the investigation was inconclusive with regard to the parties' market shares in the music stop data licensing and online advertising markets, the Commission confirmed in its investigation the existence of multiple alternative suppliers. This finding, together with the

[227] European Commission. *Case M.8788 – Apple/Shazam*. ibid., 2018, p. 8.
[228] De Rijke, B. (November 14, 2018). *Lessons from EU regulator's review of Apple/Shazam merger*. Amsterdam, Brussels. De Brauw Blackstone Westbroek. Available at: https://www.debrauw.com/legalarticles/lessons-from-eu-regulators-review-of-apple-shazam-merger/
[229] European Commission. *Case M.8788 – Apple/Shazam*. op. cit., 2018, p. 31.

complementarity of the party's data sets, led to the conclusion that the merger would not give rise to horizontal effects.

With regard to non-horizontal effects, the Commission considered the possible exclusion of competing providers of digital music streaming applications due to the acquisition of commercially sensitive information, consisting of two possible groups of practices that Apple could adopt after the transaction, which is denial or degradation, music rivals to:

a) Shazam reference mechanism as a customer acquisition channel;
b) Shazam reference engine as a feature that increases user engagement and enriches the user experience;
c) Shazam as an advertising tool;
d) Shazam as a provider of music recognition functionality in the app;
e) Shazam user data as an input to improve existing functionality or provide additional functionality in music streaming services.

Here, the Commission notes, "without prejudice to the assessment by the competent data protection authorities"[230], that such aggregation of data appears to be permitted by the General Data Protection Regulation (GDPR), as Shazam's terms of service "seem to inform" about the processing of customer information processed by Shazam.[231]

In addition, Shazam can now access data about which apps are installed on a user's Android device, because the Android Developer Guidelines allow all apps to do so.[232] On the other hand, Spotify developer terms and conditions are quite strict, imposing on developers:

> (i) only request from Spotify users the data they need to operate their app;
> (ii) not to email Spotify users without explicit consent; and
> (iii) completely and accurately disclose the privacy practices and policies they apply on their app or website. Further, Spotify's terms of service (section I, points f and h) prevent the use of Spotify's user data 'in any manner to compete with Spotify'.[233]

However, despite legal and contractual restrictions on the use of customer application information, the Commission assessed whether targeted advertising made possible by the combination of databases would likely have negative impacts on effective competition and concluded that there were no reasons. Going further, Zingales did the following analysis:

> First, the ability to access the Customer App Information on Android is not limited to Shazam and would not be limited to Apple post-Transaction (unlike for iOS). Second, the market

[230] European Commission. *Case M.8788 – Apple/Shazam*. ibid., 2018, p. 47.
[231] European Commission. *Case M.8788 – Apple/Shazam*. id., 2018.
[232] European Commission. *Case M.8788 – Apple/Shazam*. id., 2018.
[233] European Commission. *Case M.8788 – Apple/Shazam*. ibid., 2018, p. 48.

> investigation clearly indicated that the digital music streaming service market in the EEA (and in the Referring States, including Iceland where Apple Music is active) has been growing considerably, and that there are already several providers with the capability of targeting 'music enthusiasts.' Third, the Commission noted that Apple has stated its plans to change Shazam's data collection practices in order to bring them in line with Apple's industry-leading positions on privacy and, thus, to update the Shazam app for OSs other than Apple's OSs so that it will 'not send to Apple the Customer App Information unless the music streaming service of that user agrees to allow this information to be sent to Apple'.[234]

The second theory of damage contemplated by the decision is that of denial and degradation of competitors' access to Shazam's reference mechanism as a customer acquisition tool. The Commission has herein determined that even if the merged entity has the technical capacity and incentives to engage in such practices, it is unlikely that they will have the ability to exclude competing providers of digital music streaming applications and adversely affect competition.

This is because Shazam's market shares do not translate into a significant degree of market power. In fact, given the low number of record references currently coming from Shazam, it is unlikely that the effects of denial or degradation of competing providers of digital music streaming application access to Shazam's reference mechanism are unlikely to be sufficient to reduce their ability or incentives to compete.

A third theory related to the decision considered by the decision concerns the denial and degradation of competitors' access to the Shazam reference mechanism as a feature that increases engagement and enriches the experience. Here, again, the Commission notes that the merged entity would have no incentives to ban competition simply because of Shazam's limited market power and the limited relevance of the reference mechanisms in competition between digital music streaming applications.

The Commission notes that, already pre-transaction, the reference block for Apple Music has a more prominent position on iOS devices (due to an existing partnership between the merging parties), which has failed to produce significant results in user engagement. And, anyway, nothing would stop users, post-transaction, from "shazaming" songs and listening to them on rival digital music streaming apps.

A fourth and important theory of the damage in the Decision explores the possible "big data" advantage resulting from the acquisition of Shazam: Shazam data can be exploited to improve existing functionality or offer additional functionality in digital music streaming applications. Here, the

[234] Zingales, N. (December 2018). *Apple/Shazam*: Data is power, but not a problem here. Sussex Law School. Competition Policy International (CPI), EU News Presents. p. 3. Available at: https://www.competitionpolicyinternational.com/appleshazam-data-is-power-but-not-a-problem-here/#_edn1

Commission concludes that Shazam's user data does not appear to be unique and therefore can confer a significant "data advantage" on Apple after the transaction.

The Commission's assessment is based on an in-depth investigation of available data on users of digital music services using four relevant big data metrics: i.e. the variety of data that make up the dataset; the speed at which data is collected (speed); the size of the dataset (volume); and economic relevance (value). In particular, he finds that Shazam data is no more comprehensive than other datasets available on the market, is generated at a lower speed and with less user engagement, and has never been considered as a strategic asset by merging parties.

A fifth theory of the damage was that Shazam could be used to serve more effective ads, for example, through push notifications that promote Apple Music on Android devices. However, this theory was quickly dismissed because Shazam's strength in the advertising market is relatively low; and that users are always free to opt out of receiving any of the notifications in question.

However, perhaps the most elaborate theory of harm examined by the Commission is related to the possible exclusion of competing providers from ACR (Automatic content recognition) software solutions, including music recognition applications, by adopting two different types of strategies: first, by providing different levels of integration as ACR functionality between Apple Music apps and competing digital music streaming apps. Second, taking advantage of Apple's strong market position in other products or services, especially in the hardware space.

The Commission rejects the first scenario, noting the existence of several alternative ACR suppliers and endorsing the view gained during the investigation that the merger can have the positive effect of encouraging digital music distributors to partner with ACR technology providers. As regards the second scenario, the Commission recognizes the theoretically possible impact on competition of the following three practices:

a) Pre-installation of the Shazam app on Apple PCs, smart mobile devices and other platforms;
b) Increased integration of the Shazam app into Apple products and services; and
c) Reducing interoperability between Apple products and services (and specifically the microphone of Apple devices) and third-party ACR software applications and solutions.

However, the Commission understand that the concerns are not specific to a merger, as there is already a partnership and integration between Apple Siri and Shazam's ACR technology. In addition, preventing the integration of hardware by competing ACR software solution providers would be against

Apple's interest in having a multitude of applications in its ecosystem, ultimately affecting its competitiveness over other platforms. In any case, the Commission excludes any likely competitive impact of such integration, given that the parties do not have a sufficiently strong market position respectively for ACR software solution platforms and ACR software solutions.

V.3 International Cooperation, Competence as Main Issues Related to Complaints and Investigation Procedures

The European Commission has recognized the role of the US market in data analysis and technological innovation and established the initiatives of the EU-US Privacy Shield Agreement (the "Privacy Shield") in collaboration with the Federal Trade Commission and the US Department of Commerce.[235, 236]

As a regulatory framework, the Privacy Shield establishes basic rules for data transfers between the EU and the United States and binds companies voluntarily registered in the Privacy Shield to EU enforcement actions under the GDPR, including fines and injunctions.[237] If, on the other hand, a company in the U.S. is not registered with the Privacy Shield, the court will apply international judgments only if the GDPR judgment does not imply constitutional rights, rights established under federal or state laws, or public policy considerations.[238]

An illustrative example would be a U.S. media company that claimed First Amendment rights against a GDPR fine, or sentence issued by a DPA. If U.S. courts decide favoring the media company, the GDPR fine will be effectively unenforceable. As consequence, the media company can still fulfill its reputation, as other companies, after the GDPR trial, as one can see their compliance with data protection below international regulatory standards. The company may also lose significant business prospects by failing to comply with the GDPR, as other U.S. companies registered under the Privacy Shield otherwise suffer pressure to avoid doing business with the company as it exposes them to the risk of non-compliance with the GDPR.

---

[235] Schwartz, P. M., & Peifer, K-N. (January 2017). Transatlantic Data Privacy Act. *Georgetown Law Journal*, *106*(1), pp. 115-179. Available at: https://www.researchgate.net/publication/321964935_Transatlantic_data_privacy_law

[236] Nohe, P. (March 30, 2018). *The GDPR and Privacy Shield – Compliance for US Businesses*. Hashed. Available at: https://www.thesslstore.com/blog/gdpr-privacy-shield-compliance-us-businesses/ pp. 115 and 163.

[237] Privacy Shield Framework. (2016). *EU – 7 Principles of the U.S.* Washington: International Trade Administration (ITA). U.S. Department of Commerce. EU-U.S. & Swiss-U.S. Privacy Shield. Available at: https://www.privacyshield.gov/EU-US-Framework

[238] Matusevitch, V., & Telnikoff, I. (D.D.C. 1995). *Summary judgment awarded against the cause of defamation action, since it is "repugnant to the public policies of the State of Maryland and the United States"* (877 F. Supp. 1, 2). Mata v. Life Ins. Co., 771 F. Sup. 1375, 1384 (D. Del. 1991) (the court refused to recognize a foreign judgment, as the case did not comply with the due process clause of the Fourteenth Amendment); Abdullah v. Sheridan Square Press, Inc., no. 93CIV.2515 (LLS), 1994 WL 419847, at * 1 (SDNY May 4, 1994) (the cause of defamation of the action under British law is dismissed, since it opposed the jurisprudence of the First Amendment)

More than a year later, the GDPR has had varied effects in different countries: there are certain cases of GDPR application outside the EU, some countries have incorporated GDPR provisions into their national legislation and/or have obtained binding clarifications from the national DPA on the applicability of the GDPR; some have tried to regulate data processing rules based on international treaties, while others have maintained a wait-and-see attitude, taking no further steps towards harmonisation of national legislation and the GDPR. These and other questions are discussed below, in country-by-country analysis.

V.4 Excessive Data Extraction as Dominance Abuse

A breach of data protection law can also constitute a violation of unfair competition law. For some logistics companies, ride-related startups and mobility, Uber may have an unfair advantage, but this can only arise if it is proven that Uber is not complying with data protection laws. In this sense, Uber's data is also a barrier to new startups that want to compete with them.

If this happens, startups that have been affected by this domain abuse can file a complaint with the authorities and/or court and therefore the remedy should be applied. There is nothing inherently wrong with being a large company or a monopoly and, in fact, in many cases this can reflect efficiencies and benefits for consumers or businesses. Still, dominant companies have a particular responsibility not to abuse their position, protecting it, expanding it or exploiting it unfairly.

In addition, the existing antitrust application, however, can be slow, complicated and unpredictable. This can be especially problematic in the rapidly evolving digital sector.[239] On the other hand, these data can also be exposed to the public, according to a decision and after a study. Of course, this data should also be the subject of anonymity, and this can also be a way to deeply verify (as an investigation) whether it complies with the GDPR.[240]

V.5 Merges and Acquisitions

It is a reality that startups can be bought by other startups, or startups can be bought by one of the players in the gig economy. It is also a fact that one of these acquisitions sampled above may even harm a small startup born.

Following the 2014 approval of Facebook's acquisition of WhatsApp without imposing any conditions, in 2017 the EU Commission imposed a fine for integrating WhatsApp and Facebook user databases without adequately informing the EU Commission of such a choice. The merging parties were fined for providing misleading and incorrect information to the EU Commission during the 2014 review of the

[239] Lomas, N. (March 13, 2019). *Competition policy must change to help startups fight 'winner takes it all' platforms, says UK report*. Available at: https://techcrunch.com/2019/03/13/competition-policy-must-change-to-help-startups-fight-winner-takes-all-platforms-says-uk-report/

[240] Furman, J. (March 2019). *Unlocking digital competition*. Report of the digital competition expert panel. London: Open Government Licence. ISBN 978-1-912809-44-8. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

concentration affecting the concentration assessment. Decision of the EU Commission on Facebook/WhatsApp adopted on 17.5.2017, (Case M. 8228).[241]

In a 2007 case, the lack of a network effect of the merger on the websites of advertisers and publishers depended on the fact that DoubleClick, acquired by Google, was "contractually prohibited" to use the data collected in the past "to offer better targeting.[242]

On 13 November 2007, the Commission concluded that the transaction raised serious doubts as to its compatibility with the common market and the functioning of the EEA Agreement and decided to initiate proceedings pursuant to Article 6(1)(c) of the Merger Regulation. After a second phase of investigation, the Commission concluded that the concentration is likely not to significantly impede effective competition in the common market or a substantial part of it and should therefore be declared compatible with the common market and the functioning of the market. Pursuant to Article 8(1) and Article 10(2) of the Merger Regulation and Article 57 of the EEA Agreement,[243] the conclusion was that:

> DoubleClick currently does not use the data it has collected in the past to offer better targeting to new advertiser customers. This is because DoubleClick is contractually prohibited from using data created through the use of DFA except for limited purposes, none of which involves using data about user behaviour for the purpose of improving ad serving to publishers or advertisers other than the one advertiser on behalf of which the data was generated and collected.[244]

In July 2019, the Italian Competition Authority (ICA), the Italian Communications Authority and the Italian Data Privacy Authority published guidelines and policy recommendations for "big data".[245] Amid some calls for more enforcement related to so-called "killer acquisitions," the ACI recommended changes in its review standards. A "fatal acquisition" occurs when a company acquires a developing product that can compete with its own product and then terminates the development of the newly purchased product to prevent competition with its existing product.

The amendments proposed by the ACI to Law No. 287/90 would allow the revision of "murderous acquisitions" under its test "Significant Impediment to Effective Competition" (SIEC). Nevertheless, the SIEC test, adopted by the European Commission in 2004, would allow the ACI to block such an acquisition if it would lead to significant anti-competitive damage. Adding, the ICA guidelines also recommend the adoption of a value-based limit to determine ICA jurisdiction to review a

---

241 European Commission. (May 5, 2017c). *Case No. M.8228 – Facebook/WhatsApp*: imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for the supply by an undertaking of incorrect or misleading information. Commission Decision of 17.5.2017. Brussels. Available at: https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf

242 Bernal & Titcomb, op. cit., 2019, pp. 70-77.

243 European Commission. (March 11, 2008). *Case No COMP/M.4731 – Google/DoubleClick*: declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement. Commission Decision of 11/03/2008. Brussels. p. 51. Available at: https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf.

244 European Commission. *Case No COMP/M.4731 – Google/DoubleClick*. id

245 Clerckx, S., Knight, Michael, K., D'Erquelinnes, H. de La B., & Miyakawa, H. (February 28, 2020). *Worldwide*: Global Merger Control Update 2020. Available at: https://www.mondaq.com/unitedstates/Anti-trustCompetition-Law/898534/Global-Merger-Control-Update-2020

transaction, this change would allow ICA to review smaller transactions that fall below current revenue limits, as is sometimes the case in the digital sector. Other jurisdictions, including Germany, Austria and Japan, have modified their merger control rules in recent years to capture similar transactions that would otherwise not require a deposit.[246]

Meanwhile, the European Data Protection Council[247] had issued a statement a few days earlier highlighting the privacy implications of the merger ("There are concerns that the combination and accumulation of sensitive personal data about people in Europe by a large technology company may pose a high level of risk to fundamental rights to privacy and the protection of personal data"). It is reported that Commissioner Vestager said that "[we] are very careful not to see a competition problem where there is a privacy problem because, if that is the case, it is not for us". The body advising the European Commission on the implementation of EU data protection legislation has also recorded in the past that we need strong and effective data protection and that where privacy acts as a parameter of competition, competition authorities can and should get involved. The role of data and the interface between competition and privacy issues is very broad and goes beyond privacy as a parameter of competition.

Another current merging discussion is about Google/Fitbit[248]. It involves the acquisition by a giant digital platform, whose business is based on monetizing customer data through multi-targeting ads and already based on a mountain of personal data and analytics capabilities from a target with unique assets for generating data in the most sensitive of all areas. It also has been capturing biometric data (health and even emotions) 24 hours a day, every day.

This agreement is advancing in a scenario of perceived great deterioration in privacy standards, as competition between data collectors has decreased and users' attention is now channeled to very few giant "attention agents". So far, the notion that privacy is also a wide-ranging concern has been explicitly acknowledged in several key reports.[249]

Another relevant release is the work of Yves-Alexandre de Montjoye one of the co-authors of the report Crémer, De Montjoye & Schweitzer[250] and the Imperial College London Computer Privacy Group. The study showed not only that there is no tension between the pursuit of privacy and competition, but also in fact, privacy and competition are strengthened.

---

[246] European Commission. *Case No COMP/M.4731 – Google/DoubleClick*. id.

[247] European Data Protection Board (EDPB). (April 17, 2020). *Wenty-second plenary session of the European Data Protection Board*. pp 10-12

[248] Caffarra, C., & Valletti, T. (March 04, 2020). *Google/Fitbit review:* Privacy IS a competition issue. Available at: https://voxeu.org/content/googlefitbit-review-privacy-competition-issue

[249] The Furman et al. report, The Cremer et al. report, The Stigler report and several others. Furman, op. cit., 2019, s/p.

[250] Crémer, De Montjoye, & Schweitzer, op. cit., 2019, s/p.

Similarly, Valletti[251], testimony before the U.S. Congress about the very role of data for competition in the digital space says that

> privacy is at the core of the economics of many digital platforms, and competition is shaped around it. The possible degradation of consumer data protection can result from market power, and it will undermine the competitive process as well as lead to detriment to consumer welfare.

Considering the above, the Facebook/WhatsApp review has lost the real motivator of the deal – capturing millennial users and monetizing even more personal data, increasing Facebook's power in advertising markets in violation of privacy rules. That merger ended with an unconditional release after a Phase 1 review because there were no concerns about "conventional" competition - despite Facebook paying $21 billion at the time, or $55 per user. Just as Google today promises that "Fitbit's 'personal' health and wellness data will not be used for Google ads, [...]".[252]

Facebook at the time swore blindly that it would not exploit WhatsApp data and monetize the $21 billion by selling emojis - something they never really did. They were fined EUR 110 million for misleading the European Commission, but still managed to maintain, mix and exploit the data. And, critically, they achieved the goal of preventing another competing social networking platform from arising.

Six years later, there is still little certainty about the limits of market domain. Certainly, one cannot say that "privacy issues" are foreign to the evaluation of mergers in such a case today; and only a "conventional" theory of damage (overlaps and vertical links in defined product markets) can justify a competition concern.[253]

V.6 The European Solution

Considering the ongoing problems of data protection, the EU wants to set the rules for the world of technology. The European Commission[254] published on 19.2.2020 "a European data strategy":

> Citizens should be empowered to make better decisions based on insights gleaned from nonpersonal data. And that data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident.

---

[251] Valletti, T. (October 18, 2019). *House Judiciary Committee*: Subcommittee on antitrust, commercial, and administrative law. "Online Platforms and Market Power Part 3: The Role of Data and Privacy in Competition". Imperial College Business School and Imperial College London. p. 4. Available at: https://docs.house.gov/meetings/JU/JU05/20191018/110098/HHRG-116-JU05-Wstate-ValettiT-20191018.pdf

[252] Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. A. L., & Nielsen, R. K. (2018). *Reuters Institute Digital News Report 2018*. Reuters Institute for the Study of Journalism. Digital News Report. pp. 20-22.

[253] Valletti, op. cit., 2019, s/p.

[254] European Commission, op. cit., 2020, p. 2.

The European data area will give EU companies the chance to scale up the single market. Common European rules and efficient enforcement mechanisms should ensure that:

a) data can flow in the EU and between sectors;
b) European rules and values, in particular the protection of personal data, consumer protection legislation and competition law, are fully respected;
c) data access and use rules are fair, practical and clear, and there are clear and reliable data governance mechanisms;
d) there is an open but assertive approach to international data flows based on European values.

Infrastructures should support the creation of European data pools, enabling big data analysis and machine learning, in a manner consistent with data protection legislation and competition law, enabling the emergence of data-driven ecosystems.

These sets can be organized centrally or distributed; in the latter case, the data is not moved to a central location to analyze it along with other data assets. The process involves analytical tools to reach the data, not the other way around. This makes it easier to keep the data protected and ensure control over who accesses what data for what purposes. These pools can be organized centrally or distributed. Another aspect is that organizations that contribute data will receive a return in the form of increased access to other employees' data, data pool analytics results, services such as predictive maintenance services, or license fees.

While data is essential for all sectors of the economy and society, each domain has its own specificities and not all sectors are moving at the same speed. Therefore, intersectoral actions for a European data area need to be accompanied by the development of sectoral data spaces in strategic areas such as manufacturing, agriculture, health and mobility.

Several issues are preventing the EU from realising its potential in the data economy. Fragmentation between Member States is an important risk to the vision of a common European data area and to the development of a genuine single data market. Several Member States have begun with adaptations of their legal framework, such as the use of privately-owned data by government authorities, processing data for scientific research purposes or adaptations to competition law.

Others undertakings are now beginning to explore how to deal with the problems at stake. The emerging differences underline the importance of joint action in order to leverage the scale of the internal market. To accomplish it, it is necessary to progress together on the following problems: data

availability and the value of the data in use and reuse. Currently, there is insufficient data available for innovative reuse, including for the development of artificial intelligence.

Moreover, problems can be grouped according to who is the data subject and who is the user of the data, but it also depends on the nature of the data involved (i.e. personal data, non-personal data or combined data sets that combine the two). Several issues concern the availability of data for the public good.

Regarding the use of public sector information by companies (government to company - G2B data sharing), the recently revised Open Data Directive (Directive 2019/1024), as well as other industry-specific legislation, ensure that the public sector makes more data produced readily available for use, in particular by SMEs, but also for civil society and the scientific community, within the framework of independent public policy assessments.[255]

However, governments can do more. High-value data sets are often not available under the same conditions across the EU, to the detriment of the use of data by SMEs that cannot afford this fragmentation. At the same time, sensitive data (e.g. health data) in public databases is generally not made available for research purposes, in the absence of capacity or mechanisms that allow specific research actions to be performed in a manner consistent with personal data protection rules.

Another relevant aspect of digital economy is the sharing and use of privately owned data by other companies (B2B) - data sharing) as well the of privately-owned data by government authorities (business-to-government - B2G data sharing). In this field, the Commission will provide further guidance to stakeholders on the compliance of data sharing and pooling agreements with EU competition law by updating the Horizontal Cooperation Guidelines (2011/C 11/01)[256]. The Commission is also prepared to provide additional individual project-related guidance on compatibility with EU competition rules if necessary. In the exercise of its merger control powers, the Commission will carefully examine the possible effects on large-scale data accumulation competition through acquisitions and the usefulness of access or data sharing remedies to address any concerns. Such legal framework was already foreseen in the "COMPETITION POLICY FOR THE DIGITAL AGE" the author Crémer, De Montjoye & Schweitzer[257], which says the following:

> a) Data pool and sharing agreements will often be competitive: they improve data access, can address bottlenecks, and contribute to a more complete realization of the innovative potential inherent in data. Grouping data of the same type or complementary data resources can allow companies to develop new or better products or services or practice algorithms more broadly and meaningfully. However, these agreements may become anticompetitive in some situations.

[255] European Commission, op. cit., 2020, p. 8.
[256] Horizontal Cooperation Guidelines (2011/C 11/01).
[257] Crémer, De Montjoye, & Schweitzer, op. cit., 2019, s/p.

For example:

1) competitors who have denied access (or access granted only on less favourable terms) may be excluded from the market;
2) the data sharing agreement may mean an anti-competitive exchange of information, including competitive information;
3) sharing or grouping of data can discourage competitors from differentiating and improving their own data collection and analysis pipelines;
4) finally, there may be cases where granting access to data on non-FRAND terms (fair, reasonable and non-discriminatory) may result in abuse of exploitation.

The assessment of competition law will necessarily depend, inter alia, on the type of data shared, on the precise form of an agreement or set of data, as well as on the market position of the relevant parties. So far, the issue is a relatively new and little researched topic in competition law. Therefore, it is necessary to exercise the scope of the different types of data pool and subsequent analysis of their pro and anti-competitive aspects to provide more guidance. This can be done through, for example, guidance letters, "no violation" decisions under Article 10 of Regulation 1/2003, or the forthcoming revision of the Guidelines on Horizontal Cooperation.[258]

Later, a block exemption regulation on sharing and data pooling may be appropriate. (c) access to data pursuant to Article 102 of the TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION. When competitors request access to data from a dominant company, thorough analysis will be required to determine whether such access is really indispensable. In addition, the legitimate interests of both parties need to be considered.[259]

The report proposes to be careful here: it is necessary to distinguish between different forms of data, levels of access and use of data. In various configurations, access to data will not be indispensable to compete, and public authorities should refrain from intervening. Furthermore, Article 102 of the TREATY ON THE FUNCTIONING OF THE EU is not the best tool for dealing with data requests by applicants seeking commercial purposes essentially unrelated to the market served by the dominant company (i.e. access to data for training purposes).[260] Otherwise, AI algorithms for unrelated purposes in such cases seems preferable to the emergence of market-based solutions or the adoption of a regulatory regime.

There are other settings, however, in which it is necessary to impose functions to ensure access to data - and possibly interoperability of the data. This would be the case, in particular, of data requests in order to serve complementary markets or post-markets - that is, markets that are part of the broader ecosystem served by the data controller. However, in such cases, competition authorities or

[258] Crémer, De Montjoye, & Schweitzer, id.
[259] Official Journal of the European Union, op. cit., 2012, s/p.
[260] Official Journal of the European Union, id.

courts will need to specify the conditions of access. This and the concomitant need to monitor can be feasible where access requests are relatively standard and where access conditions are relatively stable. When this is not the case, in particular when a dominant undertaking is required to grant access to continuous data (i.e. to ensure interoperability of data), there may be a need for regulation - which must sometimes be sector-specific. In any case, competition law may specify the general preconditions and inform the possible regulatory regimes.

While laws and institutions may arise under data protection, national (or possibly EU) contractual law or other policy fields that can help promote efficient access to data in many contexts, competition law remains an important reference regime. Data access issues can arise in different configurations:

a) Today, companies are experimenting with different forms of data sharing and pooling. These arrangements will often be efficient and socially desirable, but they can also be anticompetitive in other situations. Competition law should try to encourage the first type and provide legal clarification on this topic as soon as possible - we recognize that this is not an easy task.
b) Dominant, data-rich companies may refuse to grant access to other companies. Currently, there is much debate and uncertainty as to when a refusal to grant access to data, including through interoperability, should be considered an abuse, as it leads to anti-competitive exclusion. In such a case, access to data may be mandatory in accordance with Article 102 of the Treaty on the functioning of the European Union.
c) In some situations, competition law may limit a dominant undertaking's access to data
d) Finally, access to data can be a problem in the context of merger control.
e) Refusals to grant access should be subject to a more elaborate assessment of Article 102 of the Treaty on the functioning of the European Union where:
f) The data controller maintains a gatekeeper position of some relevant type, i.e. access to data is essential to compete in one or more neighboring markets;
g) Data access requests for this purpose are somewhat standardized.[261]

In case of refusal to grant access to the data is found to be abusive, competition authorities or courts will need to specify the conditions of access.

In short, when competitors request access to data from a dominant undertaking, a thorough analysis will be required as to whether such access is really indispensable and, moreover, the legitimate interests of both parties need to be considered.

Even when a dominant company has a duty to grant access to data, such access can take different forms. In some cases, data portability of some kind will suffice. In other cases, there will be an obligation to ensure interoperability of the data and, therefore, the protocol, through a standard interface, the Application Programming Interface (API). Different techniques may be required to ensure

[261] European Comission, 2018.

anonymous use - in the case of personal data, or aggregate use of some kind in the case of non-personal data, in order to exclude an exchange of anticompetitive information.

The EC shall propose, as appropriate, a Data Act in 2021, with the general principle. This shall facilitate voluntary data sharing. The ruling will be applicable only where specific circumstances so require, access to data shall be mandatory, where appropriate under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions.[262]

V.7 Reaction of Portugal a (Des) Protect Small Businesses in Matters of Data Protection

The GDPR has forced all EU countries to transpire into their national law. Portugal did this in Law No. 58/2019 with a "good attempt" to protect startups in Article 37(2) and Article 38,2:

> The offences referred to in the preceding paragraph shall be punished with a fine of:
> [...]
> (b) from 1000 (euro) to 1 000 000 (euro) or 2% of annual worldwide turnover, whichever is higher in the case of SMEs;
> (c) from 500 (euro) to 250,000 (euro) in the case of natural persons. [...].[263, 264]

However, the Portuguese Data Protection Authority (CNPD) stated, under resolution 2019/494 of September 3, 2019, that nowhere in the Articles related to the sanction of the regime, there is room for an autonomous consideration of the size of the company. Therefore, the criterion adopted by the national legislator, to distinguish small and medium-sized companies to reserve the maximum monetary limit of the GDPR for large companies, constitutes in itself a violation of the GDPR.[265]

In this regard, it is important to remember that the relevance recognised in the GDPR articulated to small and medium-sized enterprises, contrary to what occurred in the initial regulatory proposal, as it was concluded in the Union institutions that the impact on personal data resulting from the conduct of those responsible for the processing of personal data (and subcontractors) does not depend on the number of workers who make up these organizations, but before the nature of the activity developed (categories of processed data, volume of data processed, categories of data subjects in processing, etc.).[266]

---

[262] European Commission, op. cit., 2020, s/p.

[263] (Diário da República Eletrônica, 2019, tradução nossa, s/p)

[264] Diário da República Eletrônica. (Agosto 08, 2019). *Lei n.º 58/2019*. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Série I. Available at: https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized

[265] Vaz, S. Q., Gonçalves, T. I., & Quartilho, J. D. (November 12, 2019). *Spain*: Portuguese Data Protection Authority declares national provisions incompatible with the GDPR. World Law Group. Available at: https://www.theworldlawgroup.com/news/portuguese-data-protection-authority-declares-national-provisions-incompatible-with-the-gdpr

[266] European Commission. (January 25, 2012). *Regulation of the European parliament and of the council*: on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (COM(2012) 11 final). Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en

As a result, the rise in Article 37(2) and Article 38(2) defines, for the illicit GDPR, different frameworks of sanctions according to the size of the undertakings. In a regulatory framework that is intended to be uniform throughout Europe, the ceilings set out in paragraphs 4 and 5 of Art. 83 of the GDPR cannot be excluded by the Member States of the Union.[267]

In fact, the legislator was not satisfied with changing the maximum fine that can be applied. He should have extended and specified the form and criteria that the fine will be applied according to the size of the company. A good example of use of data protection law is the Brazilian rule:

> Art. 52. § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> [...]
> IV - a condição econômica do infrator; [...].[268, 269]

In addition, the GDPR (2016) already provides that:

> Art. 58. Each supervisory authority shall have all of the following investigative powers:
> (a) issue warnings to a controller or processor that the intended processing operations are likely to infringe the provisions of this Regulation;
> (b) issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation;
> [...]
> (f) impose a temporary or definitive limitation, including a ban on processing;
> [...].[270]

According to Article 83, "Administrative fines shall, depending on the circumstances of each individual case, [...]measures referred to in [...] Article 58(2)". This provision leaves room to Article 58 be applied exclusively, without fines, depending on the circumstances, which could be, if the offender is a startup, for example.

---

[267] GDPR fines: how GDPR administrative fines and sanctions will be applied. (2019). I-SCOOP. Available at: https://www.i-scoop.eu/gdpr/gdpr-fines-guidelines-application-penalties/

[268] "Art. 52. § 1 - Sanctions shall be applied after administrative procedure that allows the opportunity for broad defense, gradually isolated or cumulative, according to the peculiarities of the specific case and considering the following parameters and criteria: [...] IV - the economic condition of the offender; [...]". (Câmara dos Deputados, 2018, s/p., tradução nossa)

[269] Brasil. Câmara dos Deputados. Palácio do Congresso Nacional. (Agosto 14, 2018). *Legislação Informatizada - Lei N 13.709, de 14 de agosto de 2018 - Republicação*. Brasília, DF: Câmara dos Deputados. Palácio do Congresso Nacional. Available at: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-republicacao-156213-pl.html

[270] EU - General Data Protection Regulation. (2016b). *Article 58 EU GDPR "Powers"*. Available at: https://www.privacy-regulation.eu/en/article-58-powers-GDPR.htm

VI. CONCLUSION

The theme of this work was the convergence between competition and the legal environment of data protection: protecting startups by studying a fair competition mechanism. The method adopted in the formulation of this study is in agreement with the study proposal, which is adequate through the objectives to be achieved. The development of science is based on the achievement of results that allows to validate hypotheses about a given event or fact, present in society or not.

Based on the case involving USA and Spain, it is understood that even if a fine issued by the Spanish Data Protection Authority against the US company cannot be executed, at least it is necessary to restrict the entire activity of that company in the European Union. It seems to be more effective if the competition authority participates or at least cooperates by giving its analysis on the situation, or even participating in the investigation and helping to enforce decisions.

At the same time, the GDPR should be more pro-competitive for startups, it is very clear, when you have experience and participate in an MVP construction, which cares about everything before the break-even point of the startup is a measure of success, and innovation cannot be fostered by doing so.

Of course, a breach of data protection law can also constitute a violation of unfair competition law, neither Directive 95/46 /EC (Data Protection Directive) nor the GDPR contain a final system of sanctions that would restrict competitors' right to shares under the Unfair Competition Act (UWG) and certain data protection standards have the so-called "market conduct regulation" character and may therefore trigger a breach of unfair competition law under Section 3a UWG. The overcome is that cooperation between authorities must happens and it needs to be regulated, even to ensure that one does not interfere with the other.

In the economic perspective, startups need to have a competitive advantage over the tech giants, whereas the law should have specific provisions on this type of business, but only after understanding the main aspects of the innovative processes involved.

With regard to an approach to bringing competition authorities together with data protection authorities and establishing cooperation, with specific protection for startups related to data abuse, data limit and data usage by their competitors.

It is necessary to conduct a research in a quantitative way, in order to identify and validate what startups really need, in order to understand how data can constitute a barrier or whether they are able to access all the necessary data. Startups do not have the knowledge, investment and engineers that their giant competitors have, considering the external aspects of research and development.

The Apple/Shazam decision offers reflections for the ongoing discussion on competition law reform in a data-driven environment. One argument is the difficulty of assessing market power in the presence of non-monetary prices. The Commission also expresses discomfort in using market shares as a proxy for market power in fast-growing sectors, characterized by frequent market entry and short cycles of innovation, and observes that Shazam is not a startup and that there is no record of accomplishment in entries or in disruptive innovation. Absent from this discussion, however, there is a practical examination of technology and business models, which could undoubtedly shed light on the relative quality of products offered by competitors and the possibilities of entry.

Initially, the Shazam's decision only introduces the technology in question, distinguishing between fingerprints and watermarks: in the first, quality depends on algorithms that extract recognizable data for audio signals and a large reference database, built on the source fingerprints provided by music recorders and music streaming or download service providers and music aggregators. In the latter, quality depends on algorithms intended to insert data into the audio signal and a smaller reference database, which is likely to require closer cooperation with music publishers and record labels.

Whilst ACR software solution providers rely on both technologies, it seems difficult to assess the effects of concentration without a clear picture of the relative importance of these algorithms and reference databases. This is disconcerting, as ACR software solutions are designed to become crucial guardians for the flow of information in the EU, particularly in the light of recent legislative and policy proposals requiring the adoption of content recognition technology facilities to prevent the circulation of illegal content.

Furthermore, a measure of market power such as the ability to reduce quality in that market can hardly ignore the importance of in-service advertising. This undoubtedly implies the need for an assessment of demand elasticity in reaction to increased advertising and the frequency and intensity of advertising among ACR software solution providers. It is somewhat disappointing that, although the Commission sees a problem with its estimation of market power, it does not conduct holistic research that would allow it to reach stronger conclusions. This is even more problematic, considering that Shazam's limited market power was one of the main reasons for the dismissal of the second, third and sixth of the aforementioned damage theories.

Another noteworthy aspect in this Decision is the interaction of competition and other policy objectives. Specifically, one of the concerns that led the Commission to open a second phase of investigation was inextricably linked to data protection law: it would be possible for Apple to use the

information collected through Shazam to identify customers of Apple Music's rivals and ultimately target them with advertising or marketing campaigns.

Although data protection law does not a priori prevent this direction, the assessment in this context depends on the specific conditions of the processing of personal data, including its transparency and the safeguards available to data subjects.

However, the Commission has not carried out a detailed assessment, which could mean that by approving a concentration that raises data protection concerns, it has failed to fulfil its duty to protect the rights of the EU Charter. For this reason, a welcome development in relation to this Decision is the effort of the European Data Protection Council to initiate interinstitutional dialogue, through an unprecedented statement issued during the investigation, requesting consideration of the data protection and privacy interests of individuals where one or more companies have accumulated "significant informational power".

According to recent initiatives of the European Data Protection Supervisor, the Declaration goes beyond data protection: it requires the assessment of long-term implications for the protection of the economy, data protection and consumer rights whenever a significant merger is proposed, particularly in technology sectors of the economy.

It is not yet known whether the European Commission and other competition authorities are ready to meet this challenge. In this sense, it is worth exploring the suggestion made in the Declaration that this assessment be "separate and independent or integrated into the analysis of competition". The impact assessment of digital rights should be one of the measures proposed in the competition law reform package in the digital age. Given the lack of competence of competition authorities to determine data protection, this would require the institutionalisation of a dedicated cooperation mechanism between digital regulators.

However, this should be done carefully, with an in-depth study of startup models, in order to establish a balanced proposal to give people more control over their data, give small businesses more chances to enter and thrive, and create more predictability for large digital companies.

More policy interventions to actively support startups, including a code of conduct for "the most significant digital platforms" should be created. In particular, this policy should remain based on careful consideration of evidence and economic models. Instead of relying solely on traditional competition tools, all countries should adopt a forward-looking approach that creates and enforces a clear set of rules to limit anti-competitive actions. significant digital platforms, as well as reducing the structural barriers that currently impede effective international competition.

There is nothing inherently wrong with being a large company or a monopoly and, in fact, in many cases this can reflect efficiencies and benefits for consumers or businesses. Nevertheless, dominant companies have a particular responsibility not to abuse their position, protecting it, expanding it or exploiting it unfairly. Existing antitrust enforcement, however, can often be slow, complicated and unpredictable. This can be especially problematic in the rapidly evolving digital industry.

The digital markets unit should cooperate with a wide range of stakeholders in fulfilling its role, but with new powers available to enforce solutions and monitor, investigate and penalize non-compliance.

Datasets are not rivals, which means that opening them to additional users does not decrease the amount of data available to original users or owners. Unlike a physical asset, data is easily duplicated, so it can be accessible and useful to multiple users simultaneously. However, they are excluded by contract, technical barriers, or regulation, which means that those who collect or acquire valuable consumer data do not need or may not be able to share it with others.

Exclusive data ownership, combined with a lack of consumer involvement, can lead to a lack of competitive pressure in these markets. In turn, this can prevent the benefits of feedback cycles from being fully realized or shared with consumers.

The extent to which data is of central importance to the offer, but inaccessible to competitors, in terms of volume, speed or variety, can confer a form of advantage unmatched to the historical business, making successful rivalry less likely.

This competitive advantage can arise in many digital markets. In online search, a potential rival with fewer queries to process and less data for your algorithms to get responsive search results will yield less accurate results. This will be more evident for less frequently searched queries. Consequently, users are more likely to use the existing platform (exacerbating the competition problem). Google's persistent dominance in the face of Bing competition provides some support for this theory. That said, the available evidence on this subject is somewhat confusing. Some studies have found that larger data sets can be valuable assets for predictive analytics, although they eventually reach a point where data collection returns begin to decline. Others, such as Netflix's analysis, suggest that in some markets data scale returns may be declining rapidly.

If the provider of an online platform also operates as a competitor to its business users, it will have a unique advantage in terms of the knowledge and data it has over its rival business users and its customers.

The importance of data as a barrier to entry has been a common and compelling feature in the evidence reviewed by the Panel by industry experts and stakeholders. In response to the Panel's request for evidence, the Law Society of Scotland said that because data is powerful, already large, generally global companies, which are able to use existing data effectively, have advantages in terms of maintaining their current position and even more. increasing their market share. This will inevitably represent a barrier for new entrants (without this data) or for even smaller competitors.

There are several obvious limitations in various digital platform markets that prevent consumers and businesses from freely adopting these behaviors. Some of these restrictions are inherent to markets, but others reflect the choices of established companies.

This research, combined with broader evidence gathered through extensive expert opinions, supports the conclusion that at least some of the acquisitions made by large digital companies will be problematic. Where this occurs, the implications for long-term competition and consumer well-being will be significant.

Secure access to non-personal and anonymous data: tackling the data entry barrier for smaller and younger companies while protecting privacy. The power of mass data that drives economies of scale and scope is one of the main reasons new companies struggle to compete and bring innovative services to consumers. Overcoming this barrier will allow the digital economy to remain dynamic.

The answer is to start solving these problems, is to establish an international competition system optimized for the digital world, with an international agenda to promote competition in the digital age.

Because the digital economy is global, an international agenda is needed to take full advantage of expanded competition. This will require closer cross-border cooperation between competition authorities and governments, sharing best practices and developing a common approach to issues in international digital markets.

In this sense, the UK is already considering what they call "pro-competition policy" with the aim of improving competition, not just limiting it or causing more damage.

Updated policies have the potential to promote expanded competition; traditional competition law tools need to address the challenges of the digital economy, including the application of mergers and antitrust. These policies are important, but there is a limit to how much they can accomplish. In addition, trying to solve the problems identified in digital markets by strengthening these traditional tools, can lead to unwanted and unwanted side effects.

That is why these pro-competition measures are also recommended. Instead of focusing solely on mergers or harmful corporate actions after they occur, they would actively create competition in digital markets in advance, creating structures, rules, and standards that create space for new companies to innovate and ensure fair treatment for competitors.

The main function that should be available to the digital markets unit is to seek data opening as a tool to increase competition. As already noted, companies active in the digital economy generate and maintain significant volumes of customer personal data. This data represents an asset that enables companies to engage in data-driven innovation, helping them improve their understanding of customer demands, habits, and needs.

These innovations can benefit consumers, businesses and society. However, the economies of scale and scope associated with some data reserves can create a barrier to competition, giving companies with the most comprehensive and recent data a powerful advantage. In turn, this can represent a barrier to innovation and limit the extent to which consumers benefit from new developments.

Enabling personal data mobility can provide a consumer-led tool that will increase the use of new digital services, giving companies an easier way to compete and grow in data-driven markets. However, in some markets, the key to effective competition may be to grant potential competitors access to privately held data.

Any approach to supporting this form of data sharing should also ensure the adoption of robust privacy safeguards to respect users' rights and privacy expectations. Protections in the GDPR will delete personal data unless aggregated or anonymized.

There are several platform-led initiatives to open data for broader non-commercial uses with social benefit. For example, Uber chose to release anonymous and aggregated data under the Uber Movement scheme to inform and improve infrastructure and planning decisions. Similarly, Facebook recently announced a public interest research access scheme in collaboration with the Social Sciences Research Council. These are positive steps.

Digital platforms fully rationally decide what data they will make available to other companies based on their own private interest. Companies often have a business incentive to share data - they can be sold or made available in terms that encourage other companies to participate in the platform. This is usually part of the platform's APIs. However, 75 will generally have strong business incentives not to share data in a way that allows a company to threaten the platform's position, and the control they can exercise over that share would allow it to be reduced if such a threat became significant.

On the other hand, where public data has been released, such as providing free real-time open data from Transport for London (TfL) to developers since 2009, several new businesses and products have been created, including some that compete directly with TfL's complementary services, such as Citymapper. A Deloitte survey found that the release of data opened by TfL is generating annual economic benefits and savings of up to £130 million a year. The incentives of companies to disclose their own data differ widely - but the broader public and economic benefit of access can sometimes be considerable.

Increased data sharing would promote competition and, in turn, improve market outcomes for consumers. Requiring the opening of part of the data retention legitimately obtained from an enterprise would be a significant intervention. Platforms would be reasonably concerned about the impact on their business model, the legitimacy of requiring access to a significant asset, and the impact on investment incentives in future data collection and management.

These are important factors to be carefully considered before any mandatory use of data opening as a competition tool. As a remedy, it is likely to be more interventionist than the others proposed, and greater caution is required before being used. The unit would need to base its use on any digital market on a full analytical assessment that evaluates these factors against potential benefits and considers whether less interventional solutions would produce the desired competitive outcome.

At the same time, evidence suggests that large data stocks are at the heart of the potential for some platform markets to be dominated by single players and that this domain is entrenched in order to diminish the potential for competition for the market. In these circumstances, if other solutions did not work, data opening could be the necessary tool to create the potential for new companies to enter the market and challenge an entrenched business.

Involvement with the market would be important when considering any intervention. It can be useful to use a prioritization process to do this by restricting yourself to a shortlist of potentials.

Any data opening solution should also keep the intervention to a minimum to achieve its goal. The opening of underlying raw data, which is an entry into the service, is more likely to be proportional than access to processed information, in which companies have invested even more in obtaining information and inferences from the original data.

These digital market units should have access to it as an available tool, whenever there are markets where the benefits of their use outweigh costs in order to promote competition, where they determine that this is necessary and proportionate to achieve their goals.

If implemented, data opening can take many forms and would not require data transfer between users, which could pose greater risks to privacy protection. One model would require that a dataset be shared in a controlled environment, with access granted to approved companies. This would be comparable to the UK Office for National Statistics (ONS) Secure Research Service, which provides access to unidentified data (in full compliance if GDPR rules), such as business research data, to researchers and approved government departments. ONS is able to set constraints and limits on datasets made available to users, which can combine these sets with their own, enabling data-driven insights and innovation. Under this model, the ability of approved companies to access or interrogate remains under the control of the ONS, ensuring that all privacy safeguards are preserved and that the work done is transparent. Any use would require ensuring the privacy of any personal data involved.

Experts and consultants also need to be part of the digital market unit's decisions. The digital markets unit should cooperate with a wide range of stakeholders in fulfilling its role, but with new powers available to enforce solutions and monitor, investigate and penalize non-compliance.

Taking preventative actions to limit data collection and use by antitrust regulators may not always be the right answer.

Regardless of the discussion, competitors should threaten GDPR compliance as a fair competitive advantage, but before any regulation sits, studies need to be done and the operation of the innovation process needs to be understood.

Cases cannot be treated in the same way, without confirming whether they always have the same standard, if privacy can be treated as an element of competition in all cases. Whether all merges should be treated the same way.

Finally, the present work leaves the topic open, proposing that a new research be carried out in the future, in order to contextualize the themes addressed here. Along with this new research, it is suggested to carry out a case study, for which a comparative study between European legislation on data protection law with Brazilian law is proposed.

REFERENCES

Abreu, J. C. (2018). *Interoperability solutions in the digital single market*: European electronic justice rethought under the paradigm of electronic government.

Abreu, J. C. (2019) The design of electronic justice Europe from 2019 to 2023 in the light of the Union litigation. *Anticipatory Reflections.*

Anderson, R. & Jenny, F. (2005). Competition Policy, Economic Development and the Role of a Possible Multilateral Framework on Competition Policy: Insights from the WTO Working Group on Trade and Competition Policy. Chapter 4'. In: E. Medalla (ed.). *Competition Policy in East Asia* (pp. 61-85). UK: Routledge.

Atzori, L., Iera, A. & Morabito, G. (October 28, 2010). The Internet of Things: A Survey. *Computer Networks*, *54*, Issue 15, pp. 2787-2805 2787, DOI: 10.1016. Available at: http://elsevier.staging.squizedge.net/__data/assets/pdf_file/0010/187831/The-Internet-ofThings.pdf

Aumann, R. & Hart, S. (eds.) (1994). *Handbook of Game Theory with Economic Applications* (*2*). ch. 30: "Voting Procedures" and ch. 31.

Baker, J.B. (2003). The Case for Antirust Enforcement. *Journal of Economic Perspectives*, *17*(4), pp. 27-50.

Barreneche García, A. (2013). "Analyzing the Determinants of Entrepreneurship in European Cities". *Small Business Economics*, *42*(1), pp. 77-98, DOI: 10.1007/s11187-012-9462-8.

Belitski, M. & Korosteleva, J. A. (2010). Entrepreneurial Activity Across European Cities. *Frontiers of Entrepreneurship Research*, 30.

Bernal N. & Titcomb, J. (July 16, 2019). *EU opens formal competition investigation into Amazon over use of merchant data*. San Francisco: The Elegraph.

Bernal, P. (April, 2014). *Internet Privacy Rights*: Rights to Protect Autonomy. Cambridge: Cambridge University Press.

Blank, S.; Dorf, B. (2012). *Startup*: Entrepreneur's Manual. São Paulo: Alta Books.

Blume, P. (2014). The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law*, *4*(4), p. 269-273.

Böge, U. (December 9, 2003). *Antitrust Enforcement in Europe*: The New Challenges (Merger Control). With a particular Focus on the Examination of Minority Interests under the German Merger Control Regime. (Speech at the Italian Competition Day). Rome, Italy. Available at: http://www.agcm.it/AGCM_ITA/EVENTI/EVENTI.nsf/cd33e4d549490cb4c12569 9000386c4c/37d3dc946f3f4716c1256dff005fc0ef/$FILE/UB.pdf

Bosma, N. & Schutjens, V. (2011). "Understanding Regional Variation in Entrepreneurial Activity and Entrepreneurial Attitude in Europe". *The Annals of Regional Science*, 47, 711–742. DOI 10.1007/s00168-010-0375-7.

Brasil. Câmara dos Deputados. (Agosto 14, 2018). *Legislação Informatizada - Lei N 13.709, de 14 de agosto de 2018 - Republicação*. Brasília, DF: Câmara dos Deputados/Palácio do Congresso Nacional. Available at: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-republicacao-156213-pl.html

Burgess, M. (March 24, 2020). *What is GDPR? The summary guide to GDPR compliance in the UK.* Wired. Available at: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Cabral, F. F. (maio 19, 2018). *O impacto da legislação europeia para brasileiros com negócios na internet*. Brasil: ConJur.

Caffarra, C., & Valletti, T. (March 04, 2020). Google/Fitbit review: Privacy IS a competition issue. Available at: https://voxeu.org/content/googlefitbit-review-privacy-competition-issue

Carnevale, S. G. (2018). *Europe's new data protection rules export privacy standards worldwide*. https://www.politico.eu/article/europe-data-protection-privacy-standards-gdprgeneral-protection-data-regulation/

Chang, S. J. (2004). "Venture capital financing, strategic alliances and initial public offerings of Internet startups". *Journal of*, *19*(5), pp. 721-741.

Chen, J. (Apr 24, 2017). *The New Moats*: Why Systems of Intelligence™ are the Next Defensible Business Model. Available at: https://news.greylock.com/the-new-moats-53f61aeac2d9

Clerckx, S., Knight, Michael, K., D'Erquelinnes, H. de La B., & Miyakawa, H. (February 28, 2020). *Worldwide*: Global Merger Control Update 2020. Available at: https://www.mondaq.com/unitedstates/Anti-trustCompetition-Law/898534/Global-Merger-Control-Update-2020

Colombo, M.G.; Piva, E. (January 22, 2008). Strengths and weaknesses of academic startups: a conceptual model. In: IEEE Transactions on Engineering Management. Strong and weak academic startups: a conceptual model, *55*(1), pp. 37-49. DOI: 10.1109/TEM.2007.912807. Available at: https://ieeexplore.ieee.org/document/4439878

Coppey, L. (Oct 17, 2017). *Routes to Defensibility for your Startup AI*: A simple framework for understanding the impact of data network effects and incumbents' advantages in your industry. Available at: https://machinelearnings.co/routes-to-defensibility-for-your-ai-startup-2875a1b51d4e

Craig, P. & Burca, G. (2008) EU LAW, Text, Cases and Materials (Sixth Edition, p. 1074). Oxford University Press.

Crandal, R.W., & Winston, C. (2005), 'Does Antitrust Policy Improve Consumer Welfare? Assessing the Evidence', Chapter 2. In: C. Robinson (ed.). Governments, Competition and Utility Regulation. London Business School, The Institute of Economic Affairs, Cheltenham: Edward Elgar Publishing Limited.

Crémer, J., De Montjoye, Y-A., & Schweitzer, H. (2019) *Competition policy for the digital age*. Luxembourg: Publications Office of the European Union. DOI: 10.2763/407537. Available at: https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

Cricket, I., & Irigoyen, J-M. (2006). Entrepreneurship in the EU: To wish and not to be. *Small Business Economics*, 26, pp: 305-318.

Daigle, B., & Khan, M. (September 2019). *One Year In*: GDPR Fines and Investigations against U.S.-Based Firms. U.S. International Trade Commission (USITC) Executive Briefings on Trade. Available at: https://www.usitc.gov/publications/332/executive_briefings/gdpr_enforcement.pdf

Damro, D.C. (2004). 'International Competition Policy: Bilateral and Multilateral Efforts at Dispute Prevention'. B. Hocking and S. McGuire (eds), *Trade Politics, Routledge*

Data Ethics and Innovation Consultation Centre. (November 20, 2018). Available at: https://www.gov.uk/government/consultations/consultation-on-the-centre-for-data-ethics-and-innovation/centre-for-data-ethics-and-innovation-consultation

Davila, A., Foster, G. & Gupta, M. (2003). Venture capital financing and the growth of startup firms. *Journal of Business Venturing*, *18*(6), pp. 689-708.

De Hert, P. & Papakonstantinou, V. (August 1, 2015) Comment Google Spain: Addressing Critiques and Misunderstandings One Year Later. *Maastricht Journal of European and Comparative Law*, *22*(4), p. 624.

De Rijke, B. (November 14, 2018). *Lessons from EU regulator's review of Apple/Shazam merger*. Amsterdam, Brussels. De Brauw Blackstone Westbroek.

Decker, C. (2009). *Economics and the Enforcement of European Competition Law*. Research Fellow in Law and Economics, CSLS, University of Oxford, UK: Mr. Edward Elgar Publishing. Cheltenham.

Diário da República Eletrônica. (Agosto 08, 2019). *Lei n.º 58/2019*. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Série I. Available at: https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized

Eckhardt, J. & Steffen, N. (January 16, 2019). *Is a violation of a GDPR rule at the same time a violation of competition law*? International Network of Privacy Law Professionals (INPLP). Available at: https://inplp.com/latest-news/article/is-a-violation-of-a-gdpr-rule-at-the-same-time-a-violation-of-competition-law/

Edison, H., Smørsgård, N.M., Xiaofeng, W. & Abrahamsson, P. (2018). "Lean internal startups forsoftware product innovation in large companies: enablers and inhibitors". *Journal of Systems and Software*, *135*, pp. 69-87

Essays, U. K. (2018). *Competition between companies with the same product marketing trial*. Available at: https://www.ukessays.com/essays/marketing/competition-between-companies-with-the-same-product-marketing-essay.php?vref=1

EU - General Data Protection Regulation. (2016a). *Recital 9 EU GDPR*. Available at: https://www.privacy-regulation.eu/en/r9.htm

EU - General Data Protection Regulation. (2016b). *Article 58 EU GDPR "Powers"*. Available at: https://www.privacy-regulation.eu/en/article-58-powers-GDPR.htm

EU - General Data Protection Regulation. (2016c). *Article 83 EU GDPR "General conditions for imposing administrative fines"*. Available at: https://www.privacy-regulation.eu/en/article-83-general-conditions-for-imposing-administrative-fines-GDPR.htm#5

European Commission. (2006). *Case C - 238/05 Asnef - Equifax, Solvency and Credit Information Services, SL and State Administration against the Association of Banking Users (Ausbanc)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62005CJ0238

European Commission. (2018). *Antitrust*: The Commission fined Google €4.34 billion for illegal practices related to Android mobile devices to strengthen Google's search engine dominance. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581

European Commission. (2018). Data protection: Better rules for smallbusinesses. Available at: https://ec.europa.eu/justice/smedataprotect/index_en.htm

European Commission. (2018). EU-U.S. *Privacy Shield*: Third review welcomes progress while identifying steps forimprovement. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134

European Commission. (September 6, 2018). *Case M.8788 – Apple/Shazam*. Brussels, Article 8(1), Regulation (EC) 139/2004, Commission decision of 6.9.2018. Available at: http://ec.europa.eu/competition/mergers/cases/decisions/m8788_1279_3.

European Commission. (September 6, 2018). *Case N. COMP/M.8788 - Apple/Shazam*, Commission decision. Available at: http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf

European Commission. (April 15, 2015). *Antitrust*: Commission sends statement of objections to Google in the shopping comparison service (MEMO/15/4781). Brussels. Available at: http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm

European Commission. (Feb. 19, 2020). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions*: Shaping Europe's digital future. Brussels. Available at: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

European Commission. (January 25, 2012). *Regulation of the European parliament and of the council*: on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en

European Commission. (July 25, 2014). Request for a preliminary ruling submitted by the High Court of Ireland (Ireland) on 25 July 2014 - Maximillian Schrem /Data Protection Commissioner (Case C-362/14). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CN0362

European Commission. (June 27, 2017b). *Antitrust*: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service. Brussels: European Commission - Press release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784

European Commission. (March 11, 2008). *Case No COMP/M.4731 – Google/DoubleClick*: declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement. Commission Decision of 11/03/2008. Brussels. Available at: https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf. p. 51.

European Commission. (March 2014). Regulation 2016/679 of the European Parliament and the Council of the European Union. *Official Journal of the European Communities*, 1-88. Available at: https://doi.org/http://eurlex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf

European Commission. (May 5, 2017c). *Case No. M.8228 – Facebook/WhatsApp*: imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for the supply by an undertaking of incorrect or misleading information. Commission Decision of 17.5.2017. Brussels. Available at: https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf

European Commission. (October 18, 2017a). EU-U.S. *Privacy Shield*: First review shows it works but implementation can beimproved. Brussels: European Commission - Press release. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3966

European Commission. (October 23, 2019). *EU-US Privacy Shield*: Third review welcomes progress in identifying steps for improvement. Brussels. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134

European Data Protection Board (EDPB). (April 17, 2020). *Wenty-second plenary session of the European Data Protection Board*.

European Union. (2018). Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC. General Data Protection Regulation. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

Federal Trade Commission. Protecting America's Consumers. (October 2019). *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*. Available at: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

Frederiksen, D. L. & Brem, A. (2017). "How do entrepreneurs think they create value? A scientific reflection of Eric Ries's startup approach." *International Entrepreneurship and Management Journal*, *13*(8), Issue 1, pp. 169-189.

Furman, J. (March 2019). *Unlocking digital competition*: Report of the digital competition expert panel. London: Open Government Licence. ISBN 978-1-912809-44-8. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

GDPR fines: how GDPR administrative fines and sanctions will be applied. (2019). I-SCOOP. Available at: https://www.i-scoop.eu/gdpr/gdpr-fines-guidelines-application-penalties/

Gerbrandy, A. (January 16, 2019). *Rethinking Competition Law within the European Economic Constitution*. pp. 127-142. Doi.org/10.1111/jcms.12814. Available at: https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12814

Gillibrand, K. (Feb 12, 2020). *The U.S. Needs a Data Protection Agency*. Available at: https://medium.com/@gillibrandny/the-u-s-needs-a-data-protection-agency-98a054f7b6bf

Gillibrand, Kirsten (February 13, 2020). S.3300 - Data Protection Act 2020. In: 116th Congress, 2D Session, (2019-2020). *S.3300*: To establish a Federal data protection agency, and for other purposes. In the Senate of the United States. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/3300/text

Goddard, M. (November 1, 2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, DOI: 10.2501/IJMR-2017-050, *59*(6), p. 703. Available at: https://journals.sagepub.com/doi/10.2501/IJMR-2017-050

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), pp. 68-92.

Hagberg, J., Jonsson, A. & Egels-Zandén, N. (2017). Retail digitalization: implications for physical stores. *Journal of Retailing and Consumer Services*, (39), pp. 264-269.

Herrmann, B. L., Gauthier, J. F. & Holtschke, D. et al. (2015) *The Startup Ecosystem Report Series 2015*. Available at: http://startup-ecosystem.compass.co/ser2015/

Hildebrandt, M. (2009). Privacy and Identity. In: E. Claes, A. Duff & S. Gutwirth (eds) (2006). *Privacy and the criminal law* (pp. 61-104). Antwerp/Oxford: Intersentia.

Hr-On. (May 2018). *How GDPR affects recruitment and job adverts*. Available at: https://hr-on.com/how-the-general-data-protection-regulation-changes-recruitment-and-job-adverts

Hunton Andrews Kurth. (November 21, 2018). *UK ICO Issues Warning to Washington Post Over Cookie Consent Practices*. Privacy & Information Security Law Blog, Posted in Enforcement, European Union, International. Available at: https://www.huntonprivacyblog.com/2018/11/21/uk-ico-issues-warning-washington-post-cookie-consent-practices/

Hustinx, P. (July 1-12, 2013). *EU Data Protection Law*: The Review of directive 95/46/EC and the Proposed General Data Protection Regulation. Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law.

Jerome, J. (April 1, 2019) *The GDPR's Impact on Innovation Should Not Be Overstated*. Center for Democacy & Technology (CDT). European Policy, Privacy & Data. Available at: https://cdt.org/insights/the-gdprs-impact-on-innovation-should-not-be-overstated/

Kaiser, U. S. & Müller, B. (2013). *Team heterogeneity in startups and its development over time* (Discussion Paper, 13-058). Available at: http://zinc.zew.de/pub/zew-docs/dp/dp13058.pdf

Kaisler, S., Armour, F., Espinosa, J. A. & Money, W. (Jan. 7-10, 2013). Big Data: Issues and Challenges Moving Forward. In: *Proceedings of the 46th Hawaii International Conference on System Sciences*, IEEE,

(13385077), DOI: 10.1109/HICSS.2013.645, pp. 995-1004. Available at: https://ieeexplore.ieee.org/document/6479953

Kennedy, J. (March 2017). *The myth of data monopoly*: why antitrust concerns about data are exaggerated. Information Technology & Innovation Foundation. Available at: http://www2.itif.org/2017-data-competition.pdf

Kimery, A. (Feb 27, 2020). *Senator proposes new digital privacy agency with sweeping powers*. Categories: Biometrics News, Government Services. Available at: https://www.biometricupdate.com/202002/senator-proposes-new-digital-privacy-agency-with-sweeping-powers

Knapp, A.-K., Marchand, A. & Hennig-Thurau, T. (2017). How to survive in a digital world? A comprehensive analysis of success factors for brick-and-mortar retail stores: an abstract. In: M. Stieler (Hrsg.). *Developments in marketing science*: proceedings of the Academy of Marketing Science, Creating Marketing Magic and Innovative Future Marketing Trends, 2016. Academy of Marketing Science (AMS) Annual Conference (S. 301). New York: Springer.

Kochar, P. (2009) *Critically assess the way in which Article 102 TFEU has been modernised,taking as a case study the enforcement of Article 102 TFEU against either Microsoft, Intel or Google*.

Kollmann, T., Stöckmann, C., Linstaedt, J. & Kensbock, J. (2015). European Startup Monitor (ESM). German Startup Association.

Koščík, M. (2016). *The Impact of General Data Protection Regulation on the grey literature*, *13*, pp. 42-46.

Kuhnert, J. & Leps, O. (2017). *Wohnungsgemeinnützigkeit Neue* (pp. 213-258 Springer Wiesbaden Fachmedien.

Kusters, M. (2013-2014). *Competition Law*. The Concept of Abuse in New Technologies: time for Adaptations? Belgium: KU Leuven.

Lemke, C., Brenner, W. & Kirchner, K. (2017). *Einführung in die Wirtschafts informatik*. Berlin, Heidelberg: Springer.

Lomas, N. (March 13, 2019). *Competition policy must change to help startups fight 'winner takes it all' platforms, says UK report*. Available at: https://techcrunch.com/2019/03/13/competition-policy-must-change-to-help-startups-fight-winner-takes-all-platforms-says-uk-report/

Madden, S. (May-June 2012). *From Databases to Big Data*, Massachusetts Institute of Technology, *16*, pp. 4-6. DOI Bookmark: 10.1109/MIC.2012.50. Available at: http://www.computer.org/csdl/mags/ic/2012/03/mic2012030004.pdf

Matusevitch, V., & Telnikoff, I. (D.D.C. 1995). *Summary judgment awarded against the cause of defamation action, since it is "repugnant to the public policies of the State of Maryland and the United States"* (877 F. Supp. 1, 2). Mata v. Life Ins. Co., 771 F. Sup. 1375, 1384 (D. Del. 1991) (the court refused to recognize a foreign judgment, as the case did not comply with the due process clause of the Fourteenth Amendment); Abdullah v. Sheridan Square Press, Inc., no. 93CIV.2515 (LLS), 1994 WL 419847, at * 1 (SDNY May 4, 1994) (the cause of defamation of the action under British law is dismissed, since it opposed the jurisprudence of the First Amendment)

McGrath, D. (Julho 19, 2018). *Google to Appeal Record EU Fine Over Android*. Available at: https://www.eetimes.com/google-to-appeal-record-eu-fine-over-android/#esso

Michal, S. G. (2013). "Abuse of dominance – exploitative abuses," Chapters. In: I. Lianos, & D. Geradin, (ed.). *Handbook on European Competition Law* (chapter 9, pages 385-422). Edward Elgar Publishing.

Mitretodis, A., & Euper, B. (March 9, 2020). *Interaction Between Privacy and Competition Law in a Digital Economy Part-2*. Published by Fasken Martineau DuMoulin LLP. Available at: https://www.competitionchronicle.com/2020/03/interaction-between-privacy-and-competition-law-in-a-digital-economy-part-2/

Monteleone, S. & Puccio, L. (Janeiro 19, 2017). *From Safe Harbour to Privacy Shield*: Advantages and shortcomings of the new EU-US data transfer rules. European Parliamentary Research Service.

Muşetescu, R., Dima, A. & Păun, C. (2008). *The Role of the Competition Policy in Forging the European Common Market*. Munich Personal RePEc Archive. University Library of Munich. Germany.

National Commission on Information Technology and Freedoms. (2018). *Mobile apps*: formal notices for failure to consent to the processing of geolocation data for advertising targeting purposes. Available at: https://www.cnil.fr/fr/applications-mobiles-mise-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire-2

Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. A. L., & Nielsen, R. K. (2018). *Reuters Institute Digital News Report 2018*. Reuters Institute for the Study of Journalism. Digital News Report.

Nohe, P. (March 30, 2018). *The GDPR and Privacy Shield – Compliance for US Businesses*. Hashed. Available at: https://www.thesslstore.com/blog/gdpr-privacy-shield-compliance-us-businesses/

O'Brien, R. (June 8, 2016). Privacy and security: The new European data protection regulation and its data breach notification requirements. *Business Information Review*, DOI: 10.1177/0266382116650297, *33*(2), pp. 81-84. Available at: https://journals.sagepub.com/doi/10.1177/0266382116650297

Official Journal of the European Communities. (December 16, 2002). *Council Regulation (EC) No 1/2003 of 16 December 2002*, on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003R0001&from=EN

Official Journal of the European Union. (May 20, 2003). *Commission Recommendation of 6 May 2003 on concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422) 2003/361/EC)*. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:EN:PDF

Official Journal of the European Union. (Outubro 26, 2012). *Consolidated version of the treaty on the functioning of the European Union* (C 326/390). Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF

Papadopoulos, A. (2010). *The International Dimension of EU Competition Law and Policy*. The UK: Cambridge University Press.

Paul, K. (Dec 30, 2019). *California's groundbreaking privacy law takes effect in January. What does it do*? Available at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do

Picken, J. C. (2017). "From startup to scalable enterprise: laying the foundation". *Business Horizons*, *60*(5), pp. 587-595.

Pierce, J. &, Broomell, F. (February 19, 2020). *Sen. Kirsten Gillibrand Proposes New Digital Privacy Agency*. Posted in Congress, Data Privacy, Federal Trade Commission. Available at: https://www.insideprivacy.com/united-states/congress/sen-kirsten-gillibrand-proposes-new-digital-privacy-agency/

Privacy Shield Framework. (2016). *EU – 7 Principles of the U.S*. Washington: International Trade Administration (ITA). U.S. Department of Commerce. EU-U.S. & Swiss-U.S. Privacy Shield. Available at: https://www.privacyshield.gov/EU-US-Framework

Robehmed, N. (Dec 16, 2013). *What is a startup*? Available at: https://www.forbes.com/sites/natalierobehmed/2013/12/16/what-is-a-startup/#e0b766340440

Röller, L.-H. (2005). *Economic Analysis and Competition Policy Enforcement in Europe in Modelling European Mergers*: Theory, Competition and Case Studies. Edward Elgar.

Roncolato, M. (maio 28, 2018). *Nova lei de proteção de dados da Europa*. E o efeito no Brasil. Brasil: Nexo. s/p.

Salamzadeh, A. (June 14, 2015). Innovation Accelerators: Emergence of Startup Companies in Iran (pp. 6-9). In: *60th Annual ICSB World Conference*. Dubai: UAE. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2618170

Schwartz, P. M., & Peifer, K-N. (January 2017). Transatlantic Data Privacy Act. *Georgetown Law Journal*, *106*(1), pp. 115-179.Available at: https://www.researchgate.net/publication/321964935_Transatlantic_data_privacy_law

Silva, H. S. S. (Janeiro 5, 2017) *A protecção de dados pessoais na era global*: o caso Schrems. Lisboa, 109 fl. Dissertação (Mestrado em Direito, na área de Ciências Jurídicas Forenses) - Faculdade de Direito da Universidade Nova de Lisboa. Available at: https://run.unl.pt/bitstream/10362/20567/1/Silva_2017.pdf

Sobolewski, M., Mazur, J., Paliński, M. (August 10, 2017). GDPR: A step towards a user-centric internet? *Intereconomics*, DOI: 10.1007/s10272-017-0676-5, *52*(4), pp. 207-213. Available at: https://link.springer.com/article/10.1007/s10272-017-0676-5

Stamate, A. (2011). On Some Economic Aspects of the European Competition Policy Rhetoric. *Romanian Economic and Business Review*, *6*, Issue 3, pp. 127-137.

Stylianou, K. (2016). *Help Without Borders*: How the Google Android Case Threatens to Derail the Limited Scope of the Obligation to Assist Competitors. University of Leeds, School of Law.

Tantleff, A. K. (2017). Equifax Breach Affects 143M: If GDPR Were in Effect, What Would Be the Impact? *Journal of Health Care Compliance*, *19*(5), pp. 45-46. Available at:

http://escweb.lib.cbs.dk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=126012049&site=ehost-live&scope=site

Teacher, L. (2013). *Competition Law Dissertation Topic Examples*. Available at: https://www.lawteacher.net/law-dissertation-topics/competition-law.php?vref=1

Thlemann, A., & Gonzaga, P. (November 2016). *Big data:* Bringing competition policy to the digital era – OECD Competition Division - November 2016 OECD discussion. p. 31. Available at: https://www.slideshare.net/OECD-DAF/big-data-bringing-competition-policy-to-the-digital-era-oecd-competition-division-november-2016-oecd-discussion

Thuret-Benoist, M. (June 27th, 2019*). What is the difference between personally identifiable information (PII) and personal data*? Available at: https://techgdpr.com/blog/difference-between-pii-and-personal-data/

Valletti, T. (October 18, 2019). *House Judiciary Committee*: Subcommittee on antitrust, commercial, and administrative law. "Online Platforms and Market Power Part 3: The Role of Data and Privacy in Competition". Imperial College Business School and Imperial College London. p. 4. Available at: https://docs.house.gov/meetings/JU/JU05/20191018/110098/HHRG-116-JU05-Wstate-VallettiT-20191018.pdf

Vaz, S. Q., Gonçalves, T. I., & Quartilho, J. D. (November 12, 2019). *Spain*: Portuguese Data Protection Authority declares national provisions incompatible with the GDPR. World Law Group. Available at: https://www.theworldlawgroup.com/news/portuguese-data-protection-authority-declares-national-provisions-incompatible-with-the-gdpr

Veni, J.S. (1996) EU Competition Law-Enforcement and Compliance: An Overview. *Antitrust Law Journal*, *65*, pp. 81-104.

Weiss, F. (2006) Transparency as an element of good governance in EU and WTO practice: overview and comparison. *Fordham International Law Journal*, *30*, pp.1545-1586.

Whish, R., & Bailey, D. (2012). *Competition Law* (7th Edition). Oxford: Oxford University Press.

White, A. (September 19, 2018). *Amazon probed by EU on data collection from rival retailers*. Available at: https://www.bloomberg.com/news/articles/2018-09-19/amazon-probed-by-eu-on-data-collection-from-rival-retailers

White, S. (2009). Rights of the Defense in Administrative Investigations: Access to the File in EC Investigations. *Review of European Administrative Law*, *2*, Issue 1, pp. 57-69.

Wich, R. (2018). *Competition Law* (p. 829). Oxford: Oxford University Press.

Wilks, S. (June 13, 2005). Agency Escape: Decentralization or Dominance of the European Commission in the Modernization of Competition Policy? *Governance*: An International Journal of Policy, Administration, and Institutions, *18*(3), DOI: 10.1111/j.1468-0491.2005.00283.x, pp. 431-452.

Wils, W.P.J. (2008). The Use of Settlements in Public Antitrust Enforcement: Objectives and Principles. *World Competition*, *31*(3), pp.335-352.

Wolford, B. (2020). *GDPR compliance checklist for US companies*. Available at: https://gdpr.eu/compliance-checklist-us-companies/

Žák, Č. (2017). *When preparing for GDPR, do not forget to insure*. ICT Revue. p. 32.

Zarsky, Tal Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, *47*, Iss. 4, p. 995.

Zhang, A.H. (2011). Problems in Following E.U Competition Law: A Case Study of Coca-Cola/Huiyuan. *Peking University Journal of Legal Studies*, The University of Hong Kong - Faculty of Law, *3*, pp. 96-118. Available at: http://ssrn.com/abstract=1569836

Zikopoulos, P.C., Eaton, Ch., Deroos, D., Deutsch, T. & Lapis, G. (2012*). Understanding Big Data*: Analytics for Enterprise Class Hadoop and Streaming Data. The McGraw-Hill Companies.

Zingales, N. (2010). The Hearing Officer in EU Competition Law Proceedings: Ensuring Full Respect for the Right to Be Heard? *Competition Law Review*, *7*, Issue 1, pp.129-156.

Zingales, N. (December 2018). *Apple/Shazam*: Data is power, but not a problem here. Sussex Law School. Competition Policy International (CPI), EU News Presents. Available at: https://www.competitionpolicyinternational.com/appleshazam-data-is-power-but-not-a-problem-here/#_edn1