SUMMARY OF THE BIG DATA SECTOR INQUIRY

I. Introduction

The final report of the Big Data Sector Inquiry (the "Inquiry") conducted jointly by the Italian Competition Authority ("AGCM"), the Communications Regulator ("AGCOM"), and the Data Protection Authority ("Privacy Authority"), jointly the three Authorities, was published on 10 February 2020.

In the course of the Inquiry, the relevant legal and economic literature has been reviewed and included in the analysis to provide an accurate theoretical framework. The AGCM conducted hearings with academic experts and collected contributions of numerous market operators active in sectors such as telecommunications, media, digital platforms, information technology, insurance and banking. The hearings were supplemented with several requests of information. Finally, the AGCM conducted an online survey on a sample of more than two thousand Italian users, to investigate the nonmonetary relationship between the users who provide personal data and the companies that provide digital services.

The Inquiry is divided into 5 chapters and a conclusion. Chapter 1 introduces the topics covered by the Inquiry and provides a definition and description of the characteristics of Big Data. Chapter 2 describes the main issues that emerged during the hearings and that were raised by participants in the Inquiry. It also includes some examples of the impact on operations in Italian companies. In Chapter 3, the AGCOM shows how Big Data affect the electronic communications and media sectors. Chapter 4 sets out the Privacy Authority's view on the possible impact of Big Data on legislation protecting personal data and the measures and safeguards to be taken; Chapter 5 sets out the AGCM's position on the use of Big Data and the related antitrust and consumer protection implications. Finally, the conclusion offers some policy guidelines and recommendations for the legislator.

From three different yet complementary perspectives, the Inquiry examined how Big Data is driving change: from the users who provide the data, to the companies that use Big Data and, thus, the markets. The Inquiry looked at ways to exploit potential synergies between the three Authorities and to identify the most appropriate tools for any interventions.

Data have become increasingly important in recent years, particularly in organising production and in commerce, to the extent that data are no longer simply a projection of a person in the digital world but are an economic resource in their own right. Thanks to advances in Information and Communication Technology (ICT), organisations now collect all kinds of data and process them in real time to improve their decision-making processes.

These data are stored permanently for reuse later or to build new understanding and that explains why data creation is on an exponential growth path: in 2018, 28 zettabytes (ZB) of data were created worldwide, more than ten times that of 2011: by 2025 the total volume of data is expected to reach 163 ZB. This growth, driven by the emergence of online platforms, will be further accelerated by, amongst other things, the Internet of Things and 5G applications.

The intensive and extensive use of Big Data is increasingly affecting every part of the economy and society. This use delivers undeniable benefits, in terms of new opportunities, innovation and reduced transaction costs for businesses and consumer-citizens, but comes with new risks in terms of competition, protecting personal data and information pluralism.

Specifically, since large digital operators, operating globally, have access to enormous volumes and types of data (personal and non-personal, structured and unstructured) and since they have the ability to analyse and process such data, we are seeing unprecedented forms of data exploitation for economic purposes. The value of data to profiling via algorithm is, therefore, increasing as this becomes embedded into various commercial purposes, and as it generates new concentrations of power - not only "market power" but more generally economic power. This will, without doubt, affect basic rights, competitive landscapes, pluralism and the very foundations of democratic systems. This is, therefore, a phenomenon that demands the attention of every institution that contributes to defining market governance.

The three Authorities, with their different goals, characteristics and, above all, levels of perception, strived to analyse Big Data issues in a comprehensive and effective way that combined privacy and consumer protection, competition and pluralism. The results of the Inquiry highlight how it will be difficult to face the challenges posed by the digital economy without an interdisciplinary approach and how synergies between the three Authorities, equipped with complementary tools, can be effectively achieved whilst respecting each other's missions.

After more than two years of working closely together, it became clear that the positions held by the three Authorities were not so different after all: protecting privacy as a fundamental right should not hinder dynamic competition nor innovation; appropriate regulatory measures to mitigate the market power of major digital platforms should not overshadow the risks of *ex ante* intervention in innovative markets; competition in "zero price markets" should not be examined through lenses intended for traditional markets where - albeit to a lesser degree - prices and quantities continue to play a central role.

First of all, the Inquiry highlights how reducing information asymmetry between users and digital operators during the data collection phase is a fundamental policy aim and several tools can and should contribute to it. Personal data protection laws and specific consumer

protection tools can have a significant impact on reducing this information asymmetry. The aim is to ensure that users receive adequate, precise and immediate information on why their data are collected and how they will be used, and that users are able to exercise their consumer choices knowingly and effectively. The aim is to empower consumers and citizens.

During the Inquiry it emerged that data are often processed for purposes that are defined in general terms only: indeed, the mass acquisition of data can make it difficult to specifically identify *ex ante* the purposes for such processing. Innovative solutions have been proposed to encourage the individual to participate in the processing of his/her data that uses Big Data techniques, such as dynamic consent, whereby an individual initially gives their broad consent to a general notice regarding the possible purposes for processing their data, to subsequently receive more detailed information with a request to give additional and more specific consent.

From a strictly antitrust perspective, repressing abusive conducts, particularly by big players in the digital economy, and anticompetitive agreements, both of which can be facilitated by software and sophisticated algorithms, are priorities for the AGCM. The ability to profile, taken to its extreme, and the intensification of the network effect can actually facilitate abusive behaviour by, and reduce the contestability of, the main platform ecosystems. The result can make their market power persistent, whilst the spread of pro-collusive price algorithms can create and strengthen cartels and generate market environments which facilitate collusive outcome.

In any case, the digital economy requires a new balance between the risk of discouraging innovation and the risk of under-enforcement. With this in mind, the consumer welfare objective can be achieved by not restricting the analysis to traditional parameters linked to price and quantity, but extending it to quality, innovation and fairness.

With regard to data access, synergies between competition and regulation can also be useful. Under antitrust law, a dominant company may be required to provide access to data when they meet the characteristics of an essential facility, i.e., that are indispensable and not easily duplicated, in order to safeguard competition in one or more markets in which that company operates. If, though, the aim is to protect the public interest, other than that of promoting competition, then limited regulatory measures regarding data access appear to be desirable and more effective, since they can contribute to promoting competition when antitrust measures prove insufficient. In any case, any regulatory interventions regarding access to data must be necessary and proportionate, and they must take into account the specific nature of the service/market, as well as the social aims connected to them and which are subject to regulatory supervision.

The content of any obligations to access personal data - in terms of scope, nature and manner – must, in any case, be suitably balanced with protecting personal data. In particular cases, competition law may require additional obligations, in terms of personal data mobility and portability, to those generally provided for in legislation on the protection of personal data. Such additional obligations could be implemented through the adoption of open and interoperable standards, to encourage competition in the various areas where data can be exploited economically and, consequently, to provide more effective protection for the consumer-user.

An effective public policy on Big Data and the digital economy requires not just competition enforcement, but also adequate advocacy activity in order to tackle the rules and regulations aimed, firstly, at protecting "mature" market structures at the expense of innovation driven by digitalisation, and, secondly, at contributing to the competitiveness of the economy and consumer welfare. A level playing field needs to be defined through measures aimed at removing the unjustified advantages of taxation and industrial relations benefitting the main players in the digital revolution in general and in relation to the various relevant affected markets, and in relation to the intermediated markets of the large digital platforms. What is desirable is protection for competition and not from competition. In this perspective, there is a need to emancipate the public and increase awareness of both the benefits and the risks of the digitalisation of the economy.

More generally, the challenges presented by the digital economy and by Big Data require existing synergies between *ex ante* and *ex post* tools to be exploited fully, in order to protect privacy, competition, the consumer and pluralism. In this context, there is a need (and not only domestically) for supervisory authorities to take on suitable professionals (data scientists) to ensure they can continue to fulfil their institutional tasks.

The three Authorities have committed to defining a permanent cooperation mechanism in relation to acting on and studying the impact of Big Data on businesses, consumers and citizens.

II. The AGCOM's considerations

In Chapter 3 of the Inquiry, the AGCOM shows how Big Data affect all the traditionally regulated economic sectors and how this is particularly relevant to the audiovisual media and electronic communications sectors.

Big Data indeed affects business models financed by online advertising, but it also has impact on traditional business models in a broader way, due mainly to the convergence process that allows some online platforms to move into the electronic communications market and/or media publishing sectors. For example, some platforms providing

interpersonal communication services compete with traditional operators in the electronic communications sector, whilst video sharing platforms, social media networks and search platforms compete against traditional publishers and broadcasters for the same audience and economic resources.

In the audiovisual services sector, the AGCOM acknowledges that the growth of online global platforms producing, distributing and sharing information and entertainment content, will affect its assessment of information pluralism and competition in the audiovisual media services system as well as in the advertising markets.

As far as electronic communications are concerned, the development of Big Data and its exploitation will have both direct and indirect effects on the digital ecosystem. In this perspective, the AGCOM will face challenges related to the ex-ante regulatory assessment of electronic communications markets (the definition of the relevant markets and the identification of positions of significant market power), and to safeguarding of the principles of interconnection and interoperability.

The growing importance of digital players, both in online advertising and in producing information and its consumption, has mainly come from their ability to acquire and process huge volumes of data (personal and non-personal) which, in turn, have allowed them to achieve a position of competitive advantage. This has led the AGCOM, in July 2019, to launch a market analysis to identify and assess the relevant market and to ascertain the existence of dominant positions or positions reducing pluralism in online advertising.

Besides competitive issues, the data collection market for advertising purposes has also brought to light issues related to the production and spread of misinformation *(fake news*), and content which is harmful to human dignity (*hate speech*).

The starting point is that online platforms, based on a business model driven by advertising sales, are designed to specifically capture and to hold the consumer's attention for as long as possible. Once acquired, these platforms encourage the user to interact and to make as many "actions" (e.g. *like, scroll, search,* etc.) as possible in order to store as much data as possible and of the highest quality. The result is a user profile that serves to provide personalised content, with a strong emotional impact, linked to the user's "history" of online behaviour. In this context, we see *filter bubbles* and *self-confirmation bias* characterised by a circular causation mechanism in which the user, through his/her own choices, reveals information that interests him/her. This information is then used by algorithms to influence the user's choices, confirming their views and opinions. In order to promote greater understanding of these issues, the AGCOM has set up an Expert Committee on Online Disinformation (where activities have been conducted in parallel by five working groups) and has sought cooperation from video sharing platforms on the topic of hate speech.

In the AGCOM's opinion, Big Data will also have an impact on physical communication networks, which are evolving towards increasingly high-performance architectures. The Inquiry shows that, for electronic communications companies, a future-proof network cannot ignore Big Data and Analytics, which optimise their planning processes. Only these networks favour the development of innovative services and a global interconnection characterised by a high exchange of data and information. From a regulatory point of view, traditional operators are calling for a level playing field approach, i.e. gradually bringing the responsibility requirements of the OTT/platforms closer to those of competing operators in the offline world.

From the AGCOM's point of view, monitoring the spread of the various technologies and applications of the Internet of Things, Machine-to-Machine and Artificial Intelligence, the development of 5G services and networks, and the analysis and identification of best practices on governing the collection and management of Big Data, will be essential in ensuring the successful development of innovative networks and services that impact electronic communications infrastructures.

The AGCOM also analyses the impact of Big Data in markets adjacent to the electronic communications markets, but still characterised by the extensive use of data analysis techniques and algorithms. Such markets include banking and insurance, credit reporting and data brokering. In these areas, collection of personal data might have some concerns which would justify strengthening regulatory supervision. One potential regulatory approach could be to assess the content of privacy policies on the basis of the characteristics and needs of users, assessing whether they are proportionate, so that users are better informed about how their data will be processed.

The chapter concludes by illustrating the most recent initiatives and regulatory developments at the European level aimed at strengthening the safeguards on digital platforms (the new European Electronic Communications Code set out in Directive 2018/1972, Directive 2018/1808 on audiovisual media services and EU Regulation 2019/1150).

III. The Italian Privacy Authority's considerations

Chapter 4 sets out the Privacy Authority's position on the impact of Big Data on legislation protecting personal data and the measures and safeguards to be taken.

Since unattended developments could have serious implications, not only to the individual but also to the public as a whole (and could even breach people's fundamental rights and freedoms), a growing number of studies and recommendations have been made over the years – both at the European and national levels – to understand the potential and, above

all, the ethical implications and risks of the massive collection and processing of personal and anonymous data.

The Inquiry did reveal the opportunity for fruitful interaction between independent administrative authorities and, from this point of view, the matter of protecting personal data arises. This is due to the transversal nature that characterises it, as a necessary crossroads with respect to all the regulatory areas affected by Big Data (which are not limited to the processing by private entities alone or to the impact on consumers, but should be extended to the effects on the public sphere as well).

The activities related to the use of Big Data can highlight aspects that can conflict with the fundamental basis of data protection regulations, first and foremost with the principles of lawful and fair processing. Even the principles of data minimisation, purpose limitation and storage limitation for the time strictly necessary (to achieve the purpose(s) for which the data were collected), are unsuitable for massive collections of data. Indeed, data can be originally acquired for actual needs but then used for potential future – even if only hypothetical – necessity, or to be reused for further purposes that may not always be compatible with the original ones. The use of complex algorithms with Big Data may lead to unexpected results, which might be detrimental to individual interests and may breach the principle of fairness.

There is a clear interest in monitoring this issue because, unlike traditional forms of profiling, the added value provided by Big Data lies in the ability to use both the data collected in an automated way, by "watching" the data subject, and the data collected by inference (deduced from other data using analysis techniques). This increases the potential impact on fundamental rights and freedoms. EU Regulation 2016/679, on the protection of personal data (the "GDPR"), although it does not concern itself directly with Big Data, includes provisions that address the potential risks from profiling and automated decision-making and that protect the fundamental rights of data subjects, with restrictions where Big Data could have a significant impact on individuals (see articles 5, 6, 21 and 22).

The Privacy Authority then gives an account of the generalised concern of the growing opacity of processing with Big Data techniques and stresses how the lack of information about the main characteristics of personal data processing contrasts with the fundamental principle of transparency.

With regard to the risk of re-identification based on anonymous information provided by users, the Privacy Authority reports an increasing threat of such a risk due to the ever-increasing capacity for calculation. Indeed, digital operators, starting with anonymous data and using Big Data calculation techniques, can produce *single outing* or re-identification effects, making data that were anonymous yesterday, personal data today. Therefore, those planning to use Big Data with anonymisation techniques are required to periodically carry

out an in-depth assessment of the re-identification risk, in order to assess the "robustness" of the methodologies used to render data anonymous, and to document the process followed. In the Privacy Authority's view, the most promising technique to reduce the risk of re-identification is Differential Privacy. This technique integrates the benefits of generalisation and randomisation techniques as it provides for a query-based data access mechanism and not the publication of aggregated or randomised data (sanitized data).

The Privacy Authority then focuses on compliance with the principle of purpose limitation, requiring those planning to use the data they acquire to thoroughly assess whether such use is compatible with the purpose(s) for which the actual data were collected. The mere fact that the data are made public, and therefore can be easily processed, does not justify the re-use of such data with Big Data techniques for purposes that have nothing to do with the original purposes for which the information was provided.

Equally crucial is compliance with the principle of accuracy, which aims to ensure the quality of the data collected and the appropriateness of the criteria for analysing the selected data, and compliance with the principle of data minimisation, whereby data may be collected only to the extent necessary to achieve the purpose(s) of collection. Thus, the areas in which Big Data processing techniques will be used need to be considered, since processing data that is "bulkier" and dates back in time may be more justified in certain areas (e.g. scientific medical research) and less so in others (e.g. commerce).

Furthermore, the data protection impact assessment, as provided for by article 35 of the GDPR (to which, more than likely, data processing using Big Data techniques will be subject), can allow not only to identify possible risks to individual rights, but also to highlight possible undesirable ethical or social consequences.

The use of Big Data can also affect the efficiency of the public administration. Processing based on Big Data in the public domain requires an appropriate legal basis that guarantees citizens, in addition to transparency in decision-making, the proportionality of the legal recourse to this methodology in relation to the public interest objective. It also requires the identification of adequate safeguards to be included when performing such processing, after having carefully assessed the high risks to the rights and freedoms of the data subjects.

The Privacy Authority concludes by emphasising the need for more in-depth knowledge of Big Data, for a dialogue with other institutional bodies and for an increasing use of data scientists by regulators.

IV. The AGCM's considerations

Chapter 5 sets out the AGCM's position on the use of Big Data and the related antitrust and consumer protection implications.

The AGCM first outlines the structure of the markets in which Big Data are used and three macro-categories are identified: 1) markets in which the use of Big Data has a minimal role in supplying the product/service (these are markets in which Big Data is similar to other inputs used by companies); 2) markets in which the use of Big Data can affect the conditions of the supply, in terms of quality, for example, and directly affects the supplier-user relationship; 3) markets in which Big Data are essential, being fundamental characteristics of the product/service that depend on them, in particular in terms of innovation and/or personalisation (so-called data-driven markets).

In general, beyond the acquisition of data as such, in a competitive perspective what really matters is the information and the knowledge that can be generated through Big Data (as in the case of digital agriculture). Equally important are the nature, quality and quantity of data needed to compete effectively (as in the case of online search engines), as well as the number/variety of sources (online and offline) that can be used.

The Inquiry focuses on assessing market power in digital ecosystems characterised by the exploitation of Big Data. The growing importance of data, cost structures, direct and indirect network effects, switching costs and the low diffusion of multi-homing, are elements that lead to a high degree of market concentration and the creation of barriers to entry, and can result in a "winner takes all" outcome. The market power that the so-called GAFA(M) (Google, Apple, Facebook, Amazon and Microsoft) have achieved has a systemic nature. The high concentration found in digital markets becomes more problematical the more it tends to become persistent over the years.

An important element in assessing market power is the vertical and conglomerate integration of digital operators. This amplifies the ability to capture, process and exploit data in providing services to consumers and businesses, and allows for incredibly accurate profiling. The availability of Big Data, and the ability to process them, appears to give these large platforms the opportunity to exert considerable competitive influence on several markets at once, to the extent that they are perceived as entities with considerable market power even before they have entered the market. From this perspective, the competitive constraints that can be developed on the supply side, which have traditionally been used to identify potential competitive pressure, should be given much more space in the definition of the relevant market.

Strengthening market power in data-driven markets can also come from external growth, such as acquisitions by dominant players of potentially disruptive start-ups (so-called killer acquisitions). These operations could also avoid scrutiny under merger control rules: in this respect, reform at domestic and international levels is desirable in order to allow competition authorities to fully assess merger transactions that fall below the current thresholds set for prior notification, but which could potentially restrict competition from

the outset. In terms of appropriateness, the analysis of the merger transactions needs to be suited to capturing the peculiarities of "zero price" markets, where other drivers of competition, such as the level of innovation and the quality of the services and the protection of user data, are of central importance.

The relationship between the use of personal data and competition is also analysed. Collecting and, above all, using personal data are also of interest from the perspective of competition law to the extent that the data are "economic goods" able to generate revenue.

Where a service is provided by the company "free of charge", personal data are, in fact, the main if not the only value exchanged for the service itself. The ability to decide the degree to which the use of personal data is a component of the price or quality of a service assumes (i) that users are aware that they are providing their personal data, and (ii) that users are aware of the economic value of their personal data. Such an awareness does not, however, appear to be so obvious, as can be seen from the results of the consumer survey conducted by AGCM during the Inquiry[1].

As regards data acquisition, the most disruptive impact, to be assessed in light of the principles of safeguarding personal data, turns out to the fact that providers of many online services are able to acquire information about its users above and beyond that strictly related to the object of the contract, on the basis of the consent provided by the person concerned to their data being processed for one or more specific purposes.

Data acquisition is significant for businesses insofar as it allows them to obtain information that, in turn, helps them deliver a more competitive product/service. At this stage, compliance with the privacy rules plays a key role and whilst, on the one hand, it is a prerequisite for the protection of a user's personal data, on the other hand, it may also make it more difficult for businesses which do not benefit from a direct relationship with the user to access their data. In fact, the protection of personal data can conflict with the need to encourage the circulation of data and, with it, free competition between undertakings. The right to data portability should help avoid technological lock-in and increase competition between businesses providing digital services. However, there are a number of obstacles to the effective development of data portability, linked in particular to a general lack of awareness amongst users of the existence of this right, the constraints on their mobility (also due to the presence of outside network effects) and the still uncertain boundaries of data portability, which includes only part of the data collected and processed by businesses.

Developing common data transfer standards could be key to avoiding a situation in which users only make use of their right to data portability in certain, limited circumstances.

[1] For more information, see the English version of the press release of 8 June 2018, available on the AGCM's website: https://en.agcm.it/en/media/press-releases/2018/6/alias-2497

During the Inquiry, some operators highlighted how, in order to promote the free movement of data and the development of the digital economy, a model could be developed with decentralised and alternative systems, in which users have control over the data generated through their various activities and can decide independently whether and how to pool these data for a purpose to which they attach value.

Finally, the AGCM examines data-driven behaviour that could, potentially, be significant in enforcing consumer protection and competition law.

The AGCM emphases the effectiveness of consumer protection tools – some of which have already been implemented by the Authority – against messaging service providers (guilty of forcing the user to accept new terms of service) and social media networks (accused of not providing clear and accurate information on the commercial purposes for which data are collected). Consumer protection law can, in fact, be enforced across a multitude of aspects of the relationship between operators and users during the data acquisition phase. The enforcement of consumer protection rules will not only provide direct protection for consumers, but also assume a pro-competition role to the extent that users are put in a position to (more) consciously and actively exercise their consumer choices. Last but not least, consumer protection rules can be applied regardless of the existence of market power.

The consumer protection tools are complementary to the apparatus of competition law. Indeed, it is easy to imagine situations in which undertakings make "horizontal" agreements aimed at reducing the level of privacy offered or aimed at sharing personal data. This leads to the question of whether acquiring "too much" data could amount to an exploitative abuse (with the subsequent difficulties in defining a benchmark to assess when the acquisition of such personal data is considered excessive and/or unfair) or whether it could amount to conduct that could be tackled with consumer protection tools. Furthermore, cases of exclusionary abuse may occur when the use of the data is functional to adopting behaviour with a foreclosure effect in a specific market or to extending dominance in an adjacent market. Finally, the economic value of personal data should be also considered when competition authorities review merger transactions.

The AGCM then deals with the topic of personalised services and prices, analysing the risks involved. The fact that operators, given the amount of information they hold, can direct the profiled user towards personalised content, can raise critical issues, both in terms of protecting the consumer (who may not know the extent to which the search service used by the consumer filters or adjusts the results based on the user's individual characteristics) and in terms of protecting pluralism (a high degree of personalisation in the distribution of journalistic content can reduce the level of information pluralism significantly and, as a result, the consumer's ability to access a plurality and variety of information sources).

The AGCM is also aware that profiling, taken to its extreme, can facilitate abusive behaviour and reduce the contestability of the main platform ecosystems, making their market power persistent. Moreover, the spread of price algorithms, also facilitated by the availability of large amounts of data, can create and strengthen cartels and produce market environments open to collusive outcomes.

The advent of Big Data increasingly allows businesses to collect personal data from consumers and to use algorithms to implement advanced forms of price discrimination. It should be stressed, however, that in general terms, personalised pricing can improve allocative, static and dynamic efficiency. In this scenario, as well as from the perspective of consumer protection enforcement, interventions into personalised pricing become particularly complex, as they may involve the need to compare the effects on different groups of consumers.

Finally, the chapter ends with an analysis of the main conducts that can result from the exploitation of Big Data. Such conducts may constitute possible abuses of a dominant position (and which have also been assessed by the European Commission) or anti-competitive agreements implemented through the use of pricing algorithms.

More specifically, the following abusive strategies that can be adopted through the use of Big Data are analysed:

- Refusal to deal. Article 102 of the Treaty on the Functioning of the European Union (TFEU) applies in those cases in which the holder of an essential facility refuses to deal with a party with which it competes in a downstream market. Even if the essential facility consists of data, any refusal to grant third parties access to such data raises antitrust concerns if and to the extent that it is likely to reduce competition in a complementary/downstream market. In this situation, therefore, the purpose underlying a request for access to data which are held by a dominant party assumes particular importance. The most potentially relevant requests from a competitive perspective are those relating to the data required: *(i)* to offer a product/service to the consumer in the market where the data were acquired, in competition with the (dominant) operator; or *(ii)* to compete in an adjacent market; or (*iii)* to compete in an aftermarket in which the dominant operator is active. In any case, the specificity, quantity and quality of the data may facilitate abusive behaviour, in the form of a refusal to deal, only where such data meet the stringent requirements of an essential facility.
- Other exclusionary conduct. More generally, data analysis and data processing activities (analytics, cloud computing, data storage) can facilitate the implementation of potentially more widespread exclusionary conduct. A undertaking's ability and incentive to engage in anti-competitive behaviour are also

affected by the high degree of vertical and conglomerate integration that characterises the digital ecosystem. Various forms of exclusionary conduct can take place, such as, for example: (i) leveraging the dominant position held by a firm which uses data collected in a market to unduly extend its market power through anti-competitive behaviour, such as bundling; (ii) discriminatory conduct or self-preferencing, such as that adopted by a dominant undertaking which engages in platform intermediation whilst being active as a "user" on (at least) one side of the platform; (iii) reducing rivals' data, in markets where the availability of Big Data is an important source of competitive advantage and the dominant undertaking prevents its competitors from accessing such data due to, for example, contractual constraints against the use of certain services or exclusive agreements with third parties.

- Exploitative abuse. This may originate from the undisputed market power of some operators in so-called "zero price" markets and the way in which individual data are collected. Although exploitative abuses constitute a residual part of "traditional" antitrust enforcement, their relevance in digital markets appears to be potentially more extensive. These are cases which require a clear definition of the objectives that enforcement is pursuing, especially in view of the fact that such investigations may require a balance between the well-being of users on different sides of the platform, i.e. more directly between the businesses using the platforms and end consumers.

As far as price algorithms are concerned, several elements point to such algorithms can potentially facilitate situations of collusion, more or less tacit, and, therefore, more or less lawful: a greater degree of transparency in online markets, given the wide availability of price data from competitors and other relevant information; the frequency with which prices can be adjusted, given the ability of algorithms to monitor markets in real time, and given their ability to instantly and continuously change prices; and, the development of optimal pricing strategies through machine learning.

In conclusion, the AGCM will continue to monitor the conducts of digital platforms which may potentially lead to restrictions on competition.

V. The recommendations made by the three Authorities

At the end of the joint initiatives, the AGCM, AGCOM and the Data Protection Authority have reached a common view on how to tackle the issues raised by big data. This common view formed the basis for the 11 policy recommendations reported below[2]:

1. Government and Parliament should consider implementing an appropriate legal framework that addresses the issue of effective and transparent use of personal data in relation to both individuals and society as a whole.

2. Strengthen international cooperation for the governance of Big Data.

3. Promote a single and transparent policy on the mining, accessibility and use of public data in order to draft public policies which benefit firms and citizens. Coordination between these policies and EU strategies for the EU Digital Single Market will be necessary.

4. Reduce information asymmetries between digital corporations/platforms and their users (consumers and firms).

5. Identify the nature and ownership of the data prior to processing. Moreover, the possibility of identifying the data subject on the basis of anonymized data should be assessed.

6. Promote online pluralism through new tools, transparency of content and user awareness of information provided on online platforms.

7. Pursue the goal of consumer welfare with the aid of antitrust law tools. Consumer welfare may imply the evaluation of factors other than price and quantity, such as quality, innovation and fairness.

8. Reform merger control regulation so as to strengthen the effectiveness of the authorities' intervention.

9. Facilitate data portability and data mobility between platforms through the adoption of open and interoperable standards.

10. Strengthen investigative powers of the AGCM and AGCOM outside proceedings and increase the maximum financial penalties for the violation of consumer protection law.

11. Establish a "permanent coordination" between the Authorities.

[2] The English version of the full text of the 11 policy recommendations is available at the following link: https://en.ICA.it/dotcmsdoc/pressrelease/Big%20Data_Guidelines%20and%20policy%20recommendations.pdf