Key findings of the Italian joint sector inquiry into Big Data

Enzo Marasà

Summary

1. Introduction. – 2. Considerations from the Italian Authority for Communications (AGCOM). – 3. Considerations from the Italian Privacy Authority (*Garante* or IPA). – 4. Considerations from the Italian Competition Authority (AGCM or ICA). – 5. Main takeaways from the inquiry and what to expect.

Keywords

Big Data – consumers – competition – data protection – privacy

1. Introduction

On February 10, 2020 the Italian Authorities for Communications[1], Competition[2] and Data Protection[3] published the findings of a joint sector inquiry into the field of Big Data ("Investigation")[4], which lasted almost three years. It was launched on May 30, 2017 to study the functioning and impact of Big Data on the economic, political and social environment and whether the applicable regulatory framework is suitable to address concerns for the protection of privacy, consumers and competition.

Differently from similar studies in other jurisdictions[5] – which have seen the "in silos" involvement of competition authorities separately from other regulators – the Italian Investigation is the first featuring a joint effort of the three regulators of the areas of law mainly affected by the transition from analogical to digital economy. The greater added value of the Investigation rests indeed on its interdisciplinary character and the Italian ability to mix ingredients together, valorizing each one individually and as a whole.

Definition

The expression "Big Data" is used to describe the collection, analysis and storage of a vast quantity of personal and non-personal data generated from different sources. They are characterized by four main features (referred to as "the four Vs"):

1 *Autorità per le Garanzie nelle Comunicazioni* (AGCOM).

2 *Autorità Garante della Concorrenza e del Mercato* (AGCM).

3 *Garante per la Protezione dei Dati Personali* (*Garante*).

4 Published on the AGCM's website (at this link).

5 Including, inter alia, in UK, Germany, France, Spain and Benelux countries.

Volume of the enormous quantities of data collected and processed
Variety of the many different types and sources of data gathered
Velocity of the processing and elaboration activities
Value acquired by processed and elaborated data.

Value chain
The Investigation has portrayed the value chain of Big Data as structured along three levels: *(i)* data collection (further divided by data generation, collection and retention); *(ii)* data elaboration (extrapolation, integration, analysis); *(iii)* data interpretation and decision-making.
The content of the Investigation (122 pages) is vast and articulated and it is thus impossible to thoroughly address all the issues raised in a brief format. In subsequent sections A, B and C we have distilled the key findings of each of the three authorities in their respective remits. In the final section D, we wrap up with a few conclusive observations.

2. Considerations from the Italian Authority for Communications (AGCOM)

The development of digital markets and powerful platforms does not only involve the need to investigate Big Data from a competition and regulatory standpoint but also requires analysis from a constitutional perspective. AGCOM addresses Big Data from that angle too. It also observes that market failures in the context of Big Data do not only depend from the structure of markets and dynamics of supply (e.g. market power, network externalities, economics of scale) but also from certain distorted dynamics of demand of digital content/services stemming from users (as influenced by framing, prominence, self-confirmation bias, default-bias etc.). As illustrated by studies on behavioral economics, these novel distortions may too negatively compromise a competitive environment in digital markets to the detriment of consumer choice and pluralism.
Considering its competences, the analysis of the AGCOM focuses on the impact of Big Data on: (i) the dissemination of information and the protection of fundamental rights; (ii) the functioning and role of online advertising in driving consumers' information and preferences; (iii) the regulatory framework for audiovisual services and electronic communications, with a focus on regulatory asymmetries between "over the top" players (OTTs) and traditional operators.

2.1. Dissemination of distorted and biased information and threats to democratic process

The creation and supply of informative content is deeply impacted by the advent of Big Data. The Investigation highlights that the traditional journalistic and scientific cri-

teria, which before the digital era worked as gatekeepers of objective criticism, are losing this fundamental role in the society along with their ability to curb disinformation. The concentration of digital markets in the hands of a few platforms (GAFA[6]), which in large part distribute informative content generated by a great number and variety of non-professional editors (often users themselves, or even bots and algorithms), brings to a new paradox: the great increase of sources of information caused by the digital revolution does not lead to an increase of quality and variety of information but rather the opposite. The reality is that it seems to increase polarization of views while lessening the ability of consumers to distinguish between objective information, opinion and fake news.

The AGCOM warns that these factors threaten fundamental freedoms at the very founding of the democratic process and must therefore be tackled as a priority through strong policy initiatives and – possibly – new regulatory tools.

The basic concept is that data-driven, zero-pricing digital businesses aim at capturing as much consumer attention as they possibly can (generating so called "attention markets"). Digital platforms push consumers to produce a vast array of data through proposition of attractive content and interactive functions (*like*, *scroll*, *search, etc.*). As a result, platforms profile users and provide customized content strictly related to their online "history". This may severely affect the quality and neutrality of information received by users as it leads to circular mechanisms (e.g. filter bubbles, self-confirmation bias, anchor effects, echo chambers, group thinking, etc.) in which individual users reveal the information they are prone towards through their actions. The platform's algorithm then circularly re-proposes content to the same user (or clusters of users) which confirms their opinions and beliefs.

These mechanisms isolate discussion environments and predispose favorable conditions for microtargeting disinformation campaigns on aspects which have deep political and cultural impacts. Ultimately, these campaigns would allow – through the massive collection and exploitation of data – to actively influence voters, threatening the functioning of democracy. AGCOM thus rightly observes that in the digital era effective competition and differentiation of sources in the media markets (external pluralism) is no longer enough to ensure real information pluralism and quality. To the contrary, uncontrolled multiplication of sources might even accentuate auto-selection and polarization in the research and dissemination of information (*backfire effect*) if these issues are not properly addressed.

So far, to counter these practices the AGCOM has implemented and is further promoting co-regulatory initiatives with digital operators' associations and experts aimed at setting best practices codes, creating *ex ante* quality benchmarks combined with enhanced transparency obligations, *ex post* monitoring and fact-checking, and initiatives of "digital literacy" against disinformation and hate speech. Regulatory tools already exist in the weaponry of the AGCOM[7] and are being updated to also enable monitoring and tracking of ownerships and corporate links between platforms and websites/

[6] Common acronym to refer to Google, Apple, Facebook and Amazon. GAFA(M) includes Microsoft.

[7] Like the "*Informativa Economica di Sistema*" (IES) – a mandatory monitoring system provided for by national law.

brands, including sources of financing of fake contents by online advertising. The AGCOM also warns that the contrast to disinformation online requires that similar and other regulatory initiatives be tackled at EU level; and is proactively cooperating with the European Commission and the EU network of national regulatory authorities to that end.

2.2. Big Data & Online advertising: concerns for competition and pluralism

The crucial value of data for advertising purposes, which is functional to creating specific profiles on consumption habits, pushes online platforms to capture as much consumer attention as possible through the promotion and proposition of appealing content. The data so gathered are then marketed to advertisers or intermediaries and monetized, sometimes by breaching privacy rules and fundamental rights of individuals.

Against this backdrop, in July 2019 the AGCOM, in the context of the competences assigned by sectoral legislation[8], initiated proceedings aimed at assessing the existence of dominant positions in relevant markets within the online advertising sector, as capable of hindering pluralism in the wider "Integrated System of Communications" (ISC)[9]. It is the first proceeding directly involving online platforms and the correlation between collection and profiling of data for commercial purposes. The AGCOM has wide statutory powers to impose structural remedies to remove dominant positions within the ISC (for purpose of pluralism)[10] and it intends to use it to address competitive concerns at various levels of online advertising' value chain, including collection and profiling of data.

In addition to the aspects of competition and pluralism, the AGCOM points out that the dynamics of the collection of data for advertising purposes can lead to production and dissemination of disinformation and content contrary to human dignity (hate speech, racial or sexual discrimination, violence etc.).

2.3. Regulatory asymmetries and the pursue of a level playing field between OTTs and offline players

Zero-pricing digital businesses, combined with Big Data and the high level of concentration in digital markets, may enable certain platforms to aggressively expand into traditional markets with potentially disruptive consequences. Regulatory asymmetries between OTTs and "offline" players is often a perceived cause of unfair competition as it may unlevel the playing field between them. The Investigation shows that regula-

[8] Legislative Decree no. 177/2005 (as amended from time to time) and Art. 1 of Law no. 249/97.

[9] It is a bundle of media, tlc, publishing, and advertising markets statutorily defined by Legislative Decree no. 177/2005.

[10] Art. 43 of Legislative Decree no. 177/2005.

tory asymmetry is particularly problematic for competition in the electronic communications and audiovisual services sectors. Indeed, traditional operators of these sectors are since long calling for approximation of their regulatory and liability regime to that applicable to OTTs.

Electronic communications services

According to the AGCOM's findings, the need to approximate regulatory regimes in this sector has emerged mostly with respect to the following aspects.

-Safeguarding open internet and net neutrality. The rules provided by EU Regulation 2015/2120[11] to safeguard net neutrality principles, which so far have been applied solely towards internet access providers, might have to be extended to "algorithmic" platforms operating in highly concentrated markets to guarantee transparency, fairness and neutrality in the provision of strategic digital services to other businesses[12].

-Number-based interpersonal communications. The most widely diffused interpersonal communications and messaging services using the internet (e.g. WhatsApp, Messenger, etc.) require the indirect use of a mobile number as an identifier. This feature makes their functioning in the substance equivalent to traditional telephone/SMS services, whilst according to the EU regulatory framework they cannot be characterized as electronic communications. Certain measures have been introduced at EU and national level to reduce this regulatory asymmetry[13], though OTTs still escape from general authorization's requirements and thus from access and interconnection obligations applicable to traditional telephone and networks operators.

-Data protection/retention asymmetry. The pervasive diffusion of powerful OTT platforms, combined with Big Data, has unveiled a source of competitive distortion relating to differences in the applicable data protection regimes. Stakeholders from the electronic communications industry complain that traditional operators are subject to more stringent obligations on data collection and processing compared to OTTs, disadvantaging the dynamism and quality of their offering. For instance, while traditional telephone operators are subject to new consent requirements to provide enhanced data-driven services (e.g. based on geo-localization) to their customers, OTTs may request a unique consent for a bundle of digital services including interpersonal communications.

Audiovisual services

Audiovisual operators have highlighted regulatory asymmetries with respect to OTT content aggregation or hosting platforms, which do not have editorial responsibility

[11] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015.

[12] The AGCOM notes however that Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 may have addressed some of the concerns in this respect.

[13] AGCOM refers to: (i) the introduction by Art. 1(44) of law no. 124/2017 of the obligation for operators that indirectly use national plan's numbering resources to subscribe with the Register of Operators of Communications (ROC) managed by the AGCOM; and (ii) the possibility introduced by the new EU Electronic Communications Code for Member States to impose interconnection obligations to OTTs in limited cases an under the principle of proportionality (Recitals 16, 18, 149 and Art. 61.2.*c* of EU Directive 2018/1972 of 11 December 2018).

and do not own the content (e.g. platforms like Youtube, social networks and other hosting providers).

-Access to users' data and issues of data ownership. Traditional audiovisual service/content providers, unlike OTTs, find difficult to access data generated by consumers viewing their original content through the OTTs' platforms. Such data remain in the OTT's exclusive availability even without owning and having invested in content production. This puts traditional audiovisual content providers, unless vertically integrated with OTTs, at a competitive disadvantage vis-à-vis digital platforms in acquiring new customers' data and improving content accordingly. OTTs may leverage on this advantage to enter and quickly displace traditional players in the upstream content markets. The AGCOM suggests this concern may be addressed by introducing interoperability and data portability procedures by means of contract between content providers and OTTs, provided that the contractual solution complies with GDPR's consent or legitimate interest requirements. However, considering that market forces in the digital environment may not bring to solve this concern by contractual autonomy, the AGCOM evokes the possible introduction of new regulation on ownership and control of viewers' data.

-Editorial liability of OTTs over hosted content. The AGCOM considers that by organizing, promoting and ranking aggregated content based on Big Data analytics and algorithms, OTTs may harm democracy and human dignity if not held liable for the illegal content they may diffuse. Several stakeholders have complained that the e-commerce directive[14] exempts hosting platforms from prior monitoring obligation and liability on the illegal or dangerous content they may host (unless for not removing it *ex post* once identified). The new Audiovisual Service Directive[15] recognizes in part the growing competitive pressure of OTTs (in terms of audience and advertising revenues) towards traditional audiovisual service providers in this respect. In particular, it extends certain rules typically applied to the "offline" audiovisual world – namely on protection of underaged people and wider public from violent, offensive or anyhow criminal audiovisual content – to social media and video-sharing platforms if the platforms' "essential functionality" is the provision (even by mere automatic means or algorithms) of entertainment programmes and user-generated videos[16].

3. Considerations from the Italian Privacy Authority (*Garante* or IPA)

From a privacy perspective, the IPA stresses that its task is to limit the possible impact of Big Data on people's fundamental rights by, at the same time, preserving the benefits that may come from them.

[14] Directive 2000/31/EC (see Arts. 12-15).

[15] As amended by Directive (EU) 1808/2018.

[16] See Recital 5 and the new Art. 28.*b* in Directive (EU) 1808/2018.

3.1. To what extent GDPR may help handling data protection concerns raised by Big Data

The IPA notes that the GDPR[17] does not expressly deal with, and is not entirely fit to tackle, all the issues arising from across the whole value chain of Big Data. Certain provisions applicable to the collection phase may nonetheless effectively protect data subjects from information asymmetries and, indirectly, from the risks related to profiling and automated decisions. Further, the entire processing of personal data must be carried out in compliance (*by default and by design*) with the principles of lawfulness (consent/legitimate interest), fairness, transparency, purpose/data/storage minimization, accuracy and security, which are at the foundation of the GDPR (Arts. 5-6). Nevertheless, the IPA provides no straight answers to the question whether and how the GDPR may make massive volume of data collection and processing through automated techniques, which intrinsically characterizes Big Data, compliant with these fundamental principles.

3.2. The importance of preserving quality of Big Data to ensure fair and transparent profiling

The requisites of "trustfulness" and "quality" of personal data play a decisive role to a GDPR-compliant use of Big Data in profiling individuals. In this regard, the IPA invokes effective enforcement of Recital 71 of GDPR[18]. Indeed, the added value of Big Data, compared to traditional data, consists in the possibility to extract from personal data more meaningful information to identify behavioral trends, address people's needs and predict their future decisions. This is made possible by the combined use of tracking and analytics technologies (e.g. cookies and IoTs combined with AI/algorithms) enabling the direct observations of data subjects and the automated collection of related data to infer other data/information from various datasets (e.g., by identifying recurrent statistical-probabilistic correlations). The level of accuracy in processing personal data may therefore significantly condition the digital and non-digital behavior of data subjects.

3.3. The importance to comply with transparency requirements when processing Big Data

Big Data analytics techniques are frequently accused to be opaque: often users are not

[17] Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation).

[18] Recital 71 of GDPR states that «the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons […]».

aware of which data are collected and for what purposes. Therefore, the IPA highlights the paramount relevance of the GDPR's provisions aiming at ensuring transparency, particularly those requiring to inform data subjects «of the existence of automated decision-making, including profiling, referred to in Arts. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject». In this regard, the IPA notes that a correct enforcement of the principle of transparency may also significantly affect competition in digital markets, considering that the information given to data subjects may influence consumer choice in the same way as labels on goods may do.

3.4. Complexities with anonymization and pseudonymization of Big Data

Big Data often do not involve personal data. However, the IPA stresses that it is difficult to draw a hard line between personal and non-personal data as this dichotomy does not correspond to the actual complexity of the processing of Big Data. For instance, even though the processing starts from anonymized (i.e. non-personal) data, data outputs may lead to re-identify (*singleouting*) a person by combining different datasets – and this may also occur unpredictably. In other words, Big Data widen and blur the category of personal data. It is thus crucial that data controllers implement (by default and by design) "dynamic" technical and organizational measures[19] to: (i) accurately assess whether collected data are personal; and (ii) organize processing systems to preserve from voluntary or accidental re-identification. In this regard, the IPA examines the differences between existing techniques of data *anonymization*[20] and data *pseudonymization*[21].

Anonymization seeks to prevent from: (a) isolating a person from a group; (b) linking data to a certain person in a different database; and (c) inferring new personal information from another dataset. It can be achieved by combining techniques of "randomization" (e.g. *shuffling*) and "generalization" (e.g. *crowding*). However, one must find the right trade-off to preserve the utility and value of the anonymized data[22].

Pseudonymization is a less incisive and radical measure than anonymization as it allows to keep ono-to-one correspondence of the pseudonymized data with the originator. This way, while the immediate identification of data subjects is prevented in the first instance, the collected data keep their statistical and informative value intact. However, the IPA warns that pseudonymized data are still personal data (subject to the GDPR) and therefore pseudonymization cannot substitute anonymization.

[19] As opposed to "static" ore on-off measures, "dynamic" measures entail a systematic assessment at different moments in time and scope of the processing of data.

[20] Recital 26 of GDPR sets the principle that GDPR should not apply to anonymized data.

[21] See Recital 28 and Arts. 4(5), 6(3)(e), 25 and 32(1) (a) of GDPR.

[22] The IPA makes the example of an epidemic study, which is more valuable the less the data are randomized or generalized

3.5. Application to Big Data of the principles of purpose limitation and data minimization

The Investigation highlights that the enforcement of the principles of purpose limitation and data minimization is particularly challenging in the digital era. While the GDPR expressly sets out these principles and the related obligations, it is difficult in practice to apply them to massive data collection and processing through automated techniques, which is typical of Big Data.

Purpose limitation

The IPA warns that anonymization cannot be an *escamotage* to carry out processing activities incompatible with the purpose initially declared to data subjects. Enforcing the requirement to set the initial purpose as precisely as possible may help curbing arbitrary and uncontrolled use of Big Data (i.e. without renewed data subject's consent). However, the IPA recognizes that the added value of Big Data largely relies on the possibility to use data for purposes that cannot be precisely foreseen from the outset.

Data (including risk) minimization

To address this issue, the IPA invokes the strict application the "accountability" principle[23] based on a "by design approach". Data controllers should implement appropriate policies and checking systems to ensure quality, accuracy and minimized collection of data throughout the processing and against a case-by-case analysis. To this end, the IPA recommends that controllers systematically precede the processing of Big Data by a "data processing impact assessment"[24] ("DPIA") and make the DPIA publicly available. Further, controllers should adopt "dynamic" techniques to systematically check over time whether the solutions in force are still appropriate and improve them where necessary.

4. Considerations from the Italian Competition Authority (AGCM or ICA)

The ICA first provides an overview of the structure and main characteristics of data-driven markets. It then analyses various aspects of the complex interplay between use of personal data and privacy rules with market power, consumer protection and competition law, also pointing to the role and impact of public policy on the functioning of digital markets.

[23] Accountability in the framework of the GDPR requires that data controllers must not only be responsible for, but also be able to demonstrate compliance with the principles set forth in the GDPR (Art. 5.2).

[24] Art. 35 GDPR.

4.1. Structure and main characteristics of digital, data-driven markets

The ICA observes that the need to factor Big Data in the antitrust analysis mostly arises for services that either play a central role in the digital ecosystem, to the extent that could not be provided without the use of Big Data (e.g. online advertising), or are characterized by relevant information asymmetries and by distribution and intermediation activities (e.g. financial and insurance markets, with growing relevance of automotive). While these services are usually provided in highly concentrated markets also featuring dominant players, accumulation of Big Data is only one of the several factors which contribute to such characteristics. The following factors – which are not new to antitrust analysis but have become more relevant in the digital economy – still play a critical role in explaining market power of digital platforms:

- the distinctive multi-sided structure of digital markets;
- strong investments in innovative data analytics and interpretation technologies (i.e. AI and algorithms)
- economics of scale and scope;
- network effects; and
- switching costs.

The ICA stresses that it is the cumulated effect of Big Data with all these factors that is capable of strongly conditioning the competitive dynamics of digital markets, leading to "winner takes all" or "market tipping" effects, which ultimately tend to strongly benefit first movers while disincentivizing new entrants.

4.2. Big Data as a barrier to entry

Considering the above, personal data can be characterized as a barrier to entry, according to the ICA. However, the extent to which data constitute a barrier to entry must be measured case-by-case against: (i) actual relevance of Big Data for the service in question; (ii) nature, quality and quantity of data needed to compete effectively; and most importantly (iii) number and variety of sources available to attain the information and knowledge generated by such data and which is required to compete effectively.

The Investigation indicates that, in principle, what causes grater competitive strength is not data themselves but the additional information and knowledge which is possible to extract from data. In certain markets (e.g. online search) the competitive advantage may depend on the availability of a greater volume and variety of data, which combined with well-established algorithmic and machine learning technologies generate new knowledge and improved services[25]. However, the ICA notes that in digital advertising the greater value of real-time data, which can be sourced and replicated indefinitely from various sources, may make barriers for new entrants less significant

[25] Referring to online search, the ICA also mentions the need to consider increasing and decreasing economics of scale generated by the ratio between quantity, variety and frequency of data collection, citing in this respect the European Commission's *Google Search (Shopping)* case (AT.39740).

and thus incumbent's advantage deriving from Big Data less sensitive for competition. In other contexts, raw data may be easily available in large quantity and variety and the crucial factor for gaining a competitive edge is the possession of superior and proprietary AI technologies developed through important investments in innovation. Further, some markets require both data and innovation, whilst others need data of a certain quality over quantity[26].

Overall, the ICA highlights that most datasets are somehow replicable as there are countless online and offline data available on the market for different uses, often publicly accessible[27]. Hence, it concludes that only exceptionally Big Data may constitute an "essential input" to operate on a market.

4.3. Novel characteristics of market power and new challenges for antitrust in the digital ecosystem

The ICA takes as a fact that certain strategic digital services are today controlled by dominant companies, expressly pointing to markets for online search and mobile operating systems, social networks and intermediation services in e-commerce. More in general, it points to "systemic" market power caused by the global dimension and the strategic role of *gateways* played by these services. Such role would give certain platforms a "decisive influence" on social and economic dynamics of the Internet by managing access to digital markets, visibility and reputation of third-party undertakings. In particular, the Investigation identifies the following key contributors to market power of digital platforms:

-Vertical and conglomerate integration. It is considered a distinctive characteristic of leading platforms across the Big Data value chain. Supplying a whole range of services allows these platforms to combine data generated by the same subjects from different digital sources and behaviors, and thus better profiling. This integration of data and services is deemed to entrench the power these platforms hold in every market where they operate. This feedback mechanism enables certain platforms to provide an even greater range of services and to enter new markets, gaining a competitive edge from the outset. Further, the ICA points to the strategic position held by certain platforms in supplying crucial intermediate services for acquisition and elaboration of data (e.g. hosting, cloud, analytics etc.); and to the lock-in and lock-out effects that the integration of all these services, combined with limited interoperability, may have on customers and potential competitors respectively.

-Persistency of market power. Network externalities typical of multi-sided digital platforms, combined with the availability of a large volume of detailed data on users' behaviors, apparently make the market power of certain big players difficult to contend

[26] The ICA refers digital agriculture as example of a sector where data are a key competition driver and may require all the listed characteristics. See European Commission's decision in *Bayern/Monsanto*, Case M.8084 (2018).

[27] ICA refers to European Commission's merger cases *Facebook/WhatsApp* (M.7217) and *Apple/Shazam* (M.8788), in addition to hearings of Big Tech companies.

for an indefinite timeframe, according to the ICA's findings. Such perceived persistency of market power makes the high concentration level of digital markets even more problematic, as it risks discouraging investments in innovation and preventing future market entry.

-Novelty of market power. The ICA stresses that digital economic is challenging basic and consolidated antirust concepts such as the notion of undertaking, relevant market and market power. It points to the paradox that incumbents in traditional/offline markets (e.g. physical banks or insurance companies) seem to attribute actual market power to digital operators that yet have not entered their markets. Indeed, thanks to the greater availability of Big Data and the unmatchable technical capabilities to pool and exploit data to their advantage in potentially any sector, certain platforms are perceived as being able to disrupt the existing positions and become dominant immediately after entry. Competition authorities are worried that, lacking ad hoc powers and regulatory tools to intervene before conduct being occurred, they may lose momentum to prevent the creation or strengthening of persistent dominant positions in digital markets that could be extremely difficult or too late to remedy *ex post* by means of the existing antitrust toolkit.

4.4. Market power and control of concentrations

The ICA shares with other competition authorities the concern for a gap in merger control legislation, which allows digital incumbents to acquire innovative start-up platforms or technologies before they can thrive and threaten the persistency of their market power. The targets are businesses with yet a tiny or no turnover that are however very valuable for incumbent platforms because of the strategic value of their data and their innovative potential. Where the aim of such acquisitions is not to give a chance to thrive to an innovative business, which otherwise would not have a similar growth potential, but rather to impede effective competition in digital services, they are called "killer acquisitions".

killer acquisitions may escape antitrust scrutiny because the prior notification and authorization system of most merger control regimes globally is based on market turnover thresholds, which trigger mandatory notification if exceeded by the parties of the concentration. These thresholds were set in a time where market turnover was a reasonable proxy of size and power of firms, whilst the speed of innovation of digital economy and the value of data generated by zero-pricing services was not even conceivable. The target of a killer acquisition will often not exceed the minimum turnover threshold which triggers prior notification obligation with any competition authority and will thus escape scrutiny altogether. It may also be impracticable to calculate market shares in the digital sector, considering that target's activity could be an innovative service or platform with yet no market presence.

From the substantive viewpoint, increasing market power by means of mergers and acquisitions in the digital sector poses new concerns for competition, going beyond effects of the concentration on prices. The ICA warns that, in a digital economy boosted

by zero-pricing services, quality or innovation and privacy seem the most important competition drivers, which are mostly affected by market power. Analyzing these types of effects in concentrations indeed creates new challenges for the antitrust analysis: it is not only exponentially more complicated to assess the likelihood of a harm to competition; it is also difficult to distinguish between effects on competition, which is the object of antitrust law, and effects on public objectives assigned to other authorities, e.g. the protection of privacy and of other fundamental rights.

In line with similar stances expressed by public institutions globally, the ICA pushes for both procedural and substantive changes to merger control regimes at both national and international level. First, it supports the introduction of value-based thresholds (i.e. purchase price or assets' value) in merger control regimes to detect killer acquisitions. Secondly, it calls for reviewing European Commission's criteria for the antitrust analysis of concentrations by giving greater relevance and clarity to "conglomerate effects" on competition in the digital sector (e.g. with respect to powerful platforms' ability to leverage on Big Data generated by various services to create or entrench dominance across markets).

New guidance is also needed to make complicated analysis on potential effects of mergers on non-price parameters (e.g. innovation, quality, privacy level) or on the collusive potential of pricing algorithms in concentrated digital markets. All these complications are enhanced by the difficulty of defining relevant markets in the digital economy: in this respect, the Investigation suggests that the centrality of market definition in EU competition law should not prevent or make excessively complicated to stop conducts clearly producing exclusionary effects[28].

4.5. Characterizing personal data as commodity, price or quality: impact on competitive analysis

The ICA recognizes that while characterizing personal data as price or quality may – theoretically – help assessing the effects of Big Data on competition and consumers, it is exceptionally complicated to determine a minimum benchmark or expected competitive level of privacy and thus whether platforms' conducts may cause harm to competition or consumers (e.g. by unfair "prices" or degradation of quality).

Interestingly, while the ICA observes that personal data do not usually constitute autonomous object of trade but rather an ancillary good in the demand or supply of products/services, it nonetheless analyzes the features of demand and supply of personal data as they were the autonomous object of a relevant product market. By contrast, it warns that considering personal data themselves as "commodity" or "currency" might conflict with the philosophy underlying the protection of privacy as a fundamental right.

However, considering personal data as a component of the price or, in the alternative,

[28] European Commission's top officials reported to press they are about to launch a public consultation for reviewing the 1997 Market Definition Notice to respond to the new challenges of digitization and globalization.

as a quality feature of digital products/services is deemed a helpful means to address by law the impact of the merchandise of personal data on consumer welfare and competition. Characterizing personal data as (non-monetary) price highpoints that they are often the sole economic consideration in exchange of a product/service, and this enables authorities to use EU law to protect competition and consumers in "zero-pricing" digital markets.

Nevertheless, the ICA recognizes that the relationship between quality or price and the level of privacy is not univocal. For several services and consumers, a greater collection and matching of data means a more efficient service. Further, the Investigation shows that it is difficult for consumers to assign a specific value to their personal data since it is often hidden or unpredictable. The real value of personal data may be only revealed when combined with other datasets at a given point in time, acknowledgeable only by data controllers.

Further, the "negotiability" of privacy is at odds with the low level of differentiation of privacy conditions in digital platforms' offering as well with fundamental rights relating to protection of personal data (e.g. the need to comply with Arts. 5-6 GDPR). In addition, assigning the role of price or quality to personal data may "backfire" as it entails that digital players – assuming they would differentiate their offering based on the level of privacy – could charge real money for "premium", more data-protective services, thus making privacy a "luxury for a few". In this respect, the Investigation illustrates a "privacy paradox": while the very large majority of respondents to the ICA's surveys declared their strong interest in protecting their personal data, a mere third of it refuses to give whatever requested consent – a distortion attributed to the "free effect" of the offering of digital services.

4.6. The (ambivalent) effects of privacy policy on competition

Along this line, the ICA indicates that privacy rules may have an ambivalent impact on competition. A restrictive approach to data protection may curb digital incumbent's market power but also hamper the circulation and use of data across multiple sources and thus strengthen barriers to entry. However, national experience has shown that a coordinated application of sector regulation (e.g. energy and financial) with privacy rules can lead to identify the right balance to use access to data to support the dynamics of competition[29]. A full application and enforcement of the GDPRS' provisions may thus contribute to level the playing field between digital incumbents and new entrants.

The Investigation points to three topics in privacy enforcement having a crucial impact on competition: (i) portability; (ii) ownership/management of data; and (iii) purpose limitation combined with consent requirements.

(i) Data portability. The introduction of data portability by the GDPR (Art. 20) is deemed in principle a fundamental step to reduce switching costs (i.e. lock-in risks for

[29] See in this regard Decision of the *Garante* no. 39 of 25 July 2007.

users deriving from accumulation of data with one's platform) and to incentivize "multihoming" across platforms. However, the ICA observes a few potential obstacles to full exploitation of portability. Firstly, surveys sent to consumers have revealed scarce awareness of this right and on how to use it (up to 91%). Secondly, around 40% of users show low propension to multihoming for certain services (e.g. social networks) because of the time/effort it would take or lack of real alternatives. Thirdly, different standards often cause the transfer of datasets across platform technically unfeasible or unhelpful. In this respect, the principle of portability of the GDPR applies to users' raw datasets, and not to information extracted therefrom. Indeed, the GDPR only requires interoperability of platforms' data transfer systems, which does not necessarily entail compatibility of transferor's data with the transferee's services.
(ii.) Ownership and management of data. Some experts heard by the ICA suggest that market dynamics in connection with circulation of personal data may be improved by defining property rights over personal data. Similarly, other have suggested to develop alternative legal and technical architectures for managing personal data, e.g. by passing from the current system based on "centralized" management of data by platforms to a "decentralized" system based on users' control. However, the feasibility of such a solution is conditioned by the ability of users to identify the value of their personal data, which is often not foreseeable *ex ante*.
(iii.) Data minimization, purpose limitation and consent requirements. The Investigation highlights that the massive and generalized collection of Big Data inherently conflicts with the principles of data minimization and purpose limitation, which require controllers to obtain new consent from data subjects to use their data for purposes exceeding that initially communicated. Nonetheless, it may be impossible to foresee from the outset how collected data might be used and the utility they may have. Therefore, how the consent requirement is applied in relation with the principles in question may crucially impact competition by significantly affecting the ability of digital operators to promptly expand into new services and markets. Innovative solutions like "dynamic consent" (by which data subjects should be requested to confirm or retrieve their consent based on actual use of data by controllers over time) may favor the participation of individuals in processing their personal data, reduce information asymmetries enhancing "consumers empowerment" and thus improve competitive dynamics. Dynamic consent may however require alternative architectures for ownership and management of data as well as a functional separation of platforms' activities.

4.7. Possible scope of intervention of the AGCM

The ICA Investigation confirms the ICA's determination to make any possible legal use of its wide powers to enforce competition and consumer protection law to prevent the harmful consequences that may derive by misuse or strengthening of market power in the digital environment.

Consumer protection

In the recent years the ICA has fined leading digital, zero-pricing platforms for allegedly misleading and aggressive practices on the grounds that they collected personal data of consumers in exchange of services promoted as "free", without however correctly informing on how personal data are used and monetized, irrespective of a breach of the consent requirements set forth in the GDPR[30]. It now seems also willing to monitor personalization of prices and discriminatory conducts based on tracking consumers' spending behaviors and preferences by using algorithms and Big Data techniques[31]. Personalization of services may be greatly beneficial to individual consumers and consumer welfare, though it may also become unfair if leads to harmful or obscure discrimination based on use of personal data unknown to consumers and which obstructs their ability to make informed commercial choices. Notably, to effectively pursuing and enforcing consumer protection in digital markets, the ICA calls for legislative interventions to increasing maximum fines and investigative powers in the field.

Competition law

The ICA indicates that conducts entailing the use of Big Data may constitute antirust infringements (Arts. 101 and 102 TFEU or the national equivalent) in several circumstances:

-Abusive conducts. According to the ICA, the three abuse investigations carried out by the European Commission against Google in the recent years are perfectly consistent with traditional abusive conduct. The Commission has framed the peculiarities of a digital commercial practice (e.g. discriminatory use of search algorithms) within a traditional theory of harm based on exclusionary effects. This considered, the ICA deems antitrust law sufficiently flexible to address a whole set of conducts in digital markets through an evolutionary application of existing rules and theories of harm.

Notably, while recognizing the greater complexities connected with defining relevant markets in digital economy, the ICA suggests that antitrust enforcement policy could focus more on exclusionary effects than on rigorous market definition. In the ICA's opinion, this would particularly make sense for conducts leveraging on the central role of "irreplicable" Big Data in possession of a dominant platform that could simultaneously affect a variety of markets. It however stresses that refusal to deal or provide access with respect to data must in any case satisfy the "exceptional" conditions set forth by the case law on "essential facilities" to constitute an abuse. In particular, the following aspects are indicated as relevant to assess the "indispensability" of data to compete on a certain market: (i) the personal or non-personal nature of data; (ii) whether data have been collected by the dominant undertakings with the consent of data subjects rather than generated by data analytics operations or integration of various datasets;

[30] Decision of the AGCM no. 27432 in Case PS/11112 (*Facebook-sharing data with third parties*) of 29 November 2018 (as partially upheld in appeal by the first instance administrative court TAR Lazio). A precedent in line is Decision no. 26597 in Case PS/10601 (*Whatsapp – transfer of data to Facebook*) of 11 May 2017.

[31] A trend that may be confirmed during the COVID emergency with aggressive and frequent use of interim measures by the ICA (including obscuration of websites) to stop misleading practices or price gauging by digital merchants and platforms in the e-retail of essential product or services.

and (iii) the impact of GDPR or other regulations to portability and circulation of the data concerned.
Finally, the ICA speculates on hypothetical exclusionary conducts consisting in "reducing rivals' data" (as mirroring more traditional "increasing rivals' costs"). Examples refer to making more difficult for competitors to access customers' data by imposing contractual limitations to use certain services or by means of exclusivity agreements with third parties; or other obstacles imposed to customers to use competitors' services. Exploitative abuses, though more complicated to find, are deemed to possibly arise in connection with imposition by dominant platforms of unfair or "excessive" collection of personal data. Despite admitting that it is problematic to assess the competitive level beyond which collection of personal data may be deemed unfair or excessive, the ICA indicates that exploitative abuses may apply to a broader set of circumstances in digital markets than in traditional markets.
-Restrictive agreements. The ICA reminds to mainstream theories about the potential anti-competitive effects of pricing software or algorithms used by vendors or platforms to monitor and set prices of goods and services on the Internet[32]. Such algorithms may be designed or operated by competitors with the object or effect of automatically colluding on higher resale prices, in which case traditional case law on cartels may apply unproblematically. If, otherwise, such effect were the result of tacit, anti-competitive interaction between sophisticated algorithms without human intervention and awareness (so called "robot collusion"), it could become extremely complicated to construe a "meeting of minds" or "common understanding" between competitors, as required by the established case law to find an infringement of Art. 101 TFEU.

5. Main takeaways from the inquiry and what to expect

The Investigation shows that, in the field of Big Data, privacy law and policy represent the cornerstone to the main issues affecting the protection of competition, consumers and fundamental rights (including ultimately democracy). However, privacy law has ambivalent effects on these issues and may cut both ways depending on the specific circumstances. A restrictive enforcement of data protection may raise barriers to circulation of data and competition to the detriment of new entrants, while a loosen enforcement may favor digital incumbents. There is indeed no straightforward relation between competition and use of personal data and no one-size-fits-all solution.
This said, the Investigation seems to suggest that "dynamic consent" requirements may be a possible means to address a few crucial concerns in the field of competition, media pluralism and privacy. From the perspective of privacy, dynamic consent would help restituting control of personal data to data subjects and enforcing the principle of purpose limitation. From the perspective of media regulation, it would help leveling the playing field between OTTs and traditional players by approximating regulatory asymmetries on use of customers' data. From the perspective of antitrust, dynamic

[32] One of the basic texts cited on this topic is A. Ezrachi - M.E. Stucke, *Virtual Competition – The Promise and Perils of the Algorithm-driven Economy*, London, 2016.

consent could curb market power of digital incumbents by constraining their ability to leverage on Big Data accumulated across a variety of sources and services to cement their dominance into existing or new markets.

Further, dynamic consent architectures, by giving consumers better control on their data, may raise a barrier to supply-side substitutability between different digital services, thus contributing to functional separation of platform's activities. This in turn would help shaping and distinguishing relevant markets in the digital ecosystem, thus preserving rigorous market definition as a foundation of EU antitrust analysis. In this respect, various authorities across the EU, including the ICA, have proposed to loosen the centrality of market definition to better address abuse and concentration cases in digital markets. However, this stance could undermine certainty and predictability of antitrust law, ultimately making it prone towards non-economic or political considerations.

In the field of media and communications, coordinated legislative and regulatory updates along with changes to the GDPR may be necessary to develop new data ownership's architectures, which in turn would help level the playing field between OTTs and "offline" operators. For example, the rules on portability and circulation of data must be coordinated with consent and purpose limitation requirements as well as with specific consent requirements prescribed by sector regulation.

The Investigation makes evident that in-silos application of sectoral legislations by different authorities and countries is an obstacle to effectively remedy to concerns raised by Big Data on competition, consumer welfare and data protection. Given the global scale of digital players and the imperative of the Single Market within the EU, the raised issues cannot be tackled through a fragmented approach along sectoral or national lines. A holistic, synergic and harmonized application of different fields of law across jurisdictions, which combines sector regulation and common constitutional principles, has become increasingly indispensable. A few months after the conclusion of the Investigation, the European Commission launched public consultations on new ex ante regulatory measures and a New Competition Tool[33], which seem to address these concerns within such a perspective.

At the same time, competition law has its own limits and should not be used to achieve public goals that pertain to other legislative fields or political objectives. Arbitrarily using competition, consumer protection or privacy law to address one another's concerns may indeed cause conflicts of competences between authorities and the risk of double jeopardy [34]. To avoid the risk of conflicts of competences and double jeopardy in the field of Big Data, undertakings should be given the opportunity to defend within

[33] A high level and neutral summary of the rationale and possible content of the proposed measures is available in this article from the author. Another independent, academic analysis of the scope and purpose of the measures was published by Prof. Pablo Ibanez Colomo on the *Chilling Competition* blog (at this link).

[34] n the 2012 Toshiba judgment (Case C-17/10), the ECJ set out three cumulative conditions for the *ne bis in idem* principle to apply in the competition field, in contrast with the two applying to criminal matters. Accordingly, two prosecution cases have to cover the same facts, the same offender and the "same protected legal interest". However, in its Opinion rendered in a subsequent case (C-617/17), AG Wahl took the view that including the identity of the legal interest as a requisite to apply the *ne bis in idem* principle to the competition field is no longer justified.

a single proceeding from interconnected allegations investing multiple infringements potentially falling under the remits of two or more authorities. In this perspective, procedural reforms in the direction of further integrating the complementary competences and skills of competition, consumer and privacy authorities, without depriving each of their own competences, may make sense.

The ability to make case-by-case analysis also seems increasingly indispensable to avoid mistakes in the assessment of infringements. This requires that competent authorities be equipped with the right technical expertise (e.g. data scientists and analysts) to make complex analysis. Certainty of law, and thus consistency and predictability, must be safeguarded too as a fundamental right to be preserved – and this is probably the real challenge posed by Big Data.

Currently, the ICA is investigating Amazon and Google for anticompetitive practices in the markets of e-commerce intermediation services and e-mobility services respectively. It alleges – inter alia – that the two platforms may be leveraging on Big Data acquired on dominated markets to preserve prominence of their own or affiliated partners' products, thus marginalizing potential competitors[35]. For the upcoming future, the AGCM is studying competitive threats raised by Big Data in the banking, insurance and automotive sector. In addition, the Authority for Communications (AGCOM) has strong *ex ante* regulatory powers in the field of control of media and pluralism by which, theoretically, it could impose structural or behavioral remedies in the online advertising sector, which is currently under inquiry by the same AGCOM. These are crucial cases to understand future competition enforcement policy in Italy on matters such as market definition and remedies in the field of Big Data.

The impact of COVID-19 on digital economy/Big Data was not considered by the Investigation as it was closed before the outbreak. Community lockdowns are likely to further increase the importance of digital services and Big Data, thus enhancing market power of digital platforms. However, competition authorities may adapt their enforcement policy accordingly. It is conceivable that the urgent and overriding objective to protect health, safety and the well-being of the general public – particularly vulnerable peoples – may extend the scope and reach of antitrust enforcement by inflating the concept of consumer welfare, pushing competition authorities to pursue conduct that otherwise would be at the boundaries of its remit.

Hence, while waiting for the New Competition Tool, and by making a virtue of necessity, the ICA may be more resolute in testing aggressive theories of harm and enforcement against market power of digital incumbents, including by resorting to interim measures any time an immediate threat to weakened businesses or consumers is detected.

[35] A summary of the ICA's preliminary concerns is available here and here.