UiO : Faculty of Law
University of Oslo

Profiling and Online Behavioural Advertisement Under the GDPR

Has the new Regulation succeed in assuring the protection of fundamental rights without hindering innovation and economic interests in the digital economy?

Candidate number: 8027

Submission deadline: 01/12/2016

Number of words: 15.633

Abstract

The emergence of new forms of interactions in the online environment, as social media, search engine and e-commerce has shifted the business industry and introduced a data-driven economy, where data has become the new commodity. As a consequence, agents engaged in commercial activities have been collecting massive data from internet users, for instance, to predict consumer behaviour and to place tailored advertisement based on the users' interests.

Online behavioural advertisement can be legitimate and it has an important role in the digital economy, as it supports the offer of free services and it can result in better services and products to be offered to consumers. On the other hand, it raises privacy and data protection concerns, as it involves massive collection and processing of data by different agents.

The legal treatment of profiling for online behavioural advertisement shall substantially change with the introduction of the new General Data Protection Regulation, which brings new provisions for processing personal data, particularly in the online environment. Given the relevance of the new Regulation, its legislative process was surrounded by pressure and lobby by privacy authorities and industry. The final result of the Regulation is a long and complex framework, which imposes several new obligations to the companies, whereas user's rights are substantially strengthened. However, privacy advocates argue that the final text of the Regulation could be better in terms of protecting users.

The purpose of this work is to analyse whether: i) the final text GDPR provides an efficient protection of privacy and data protection in the digital context and; ii) whether the GDPR offers the agents engaged on online behavioural advertisement some level of flexibility on their business activities, insofar as they can explore the economic potentials of a data-driven economy.

Table of contents

1 INTRODUCTION

We live in a digital society, in which more often people perform their activities in the online environment. Social media, e-commerce, search engine, online education and new methods of research have changed the behaviour of the society and how companies conduct business. For instance, the marketing segment has changed significantly due to the deployment of new technologies. According to specialists, more has happened in the advertising industry in the last 2 years than in the previous 50[1]. While advertisements were previous targeted to a group of people, nowadays companies are able to offer tailored advertisement, based on the previous study of consumer's behaviour.

Such change was made possible through the deployment of new methods designed to collect and analyse data generated in the Internet. Data has become a commodity and arguably the "new oil". Thus, collection of massive data may allow companies to understand consumer behaviour and patterns and, consequently, to develop new services and products based on such studies of profiles.

Although the business model based on the collection and analysis of data has a huge economic potential, it has raised several controversies in terms of privacy. Privacy advocates argue that the new methods developed by the industry have serious impacts on the fundamental rights of privacy and data protection, as companies have been collecting and processing personal data without adequate consideration on the rights of individuals[2]. Profiling for marketing purposes is, therefore, part of a contentious debate.

Aiming to update the rules currently in force, the European Union has passed a new regulation[3] to replace the Data Protection Directive (DPD)[4], the so-called General Data Protection Regulation (GDPR or Regulation). Unlike the DPD, the Regulation is applicable to all Member States, without the need of transposing it into national law.

Given the relevance of the Regulation to both, industry and privacy advocates, the legislative process of the Regulation was long, complex and heavily lobbied. The proposal introduced by the Commission has gone through 4000 amendments in the Parliament and several other

---

[1] The Economist "Little Brother, Special Report on Advertising and Technology" 13.09.2014, http://ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

[2] King, Nancy, Profiling based on mobile, online behavior: a privacy issue, 2010, http://oregonstate.edu/ua/ncs/archives/2010/dec/profiling-based-mobile-online-behavior-privacy-issue.

[3] Regulation (EU) 2016/679.

[4] Directive 95/46/EC.

changes were introduced by the Council. The negotiations during the trialogue have taken years and the final text of the Regulation is substantially different from the proposal of the Commission[5].

The complexity of the legislative process evidences the challenges on balancing privacy and data protection with economic interests in the digital context. Thus, it is fair to say that one of the main challenges of the Regulation was to find the equilibrium on the treatment of relevant but antagonistic interests.

Privacy and data protection are fundamental rights, whereas innovation and economic interests are not expressly referred as fundamental right in the Charter of Fundamental Rights. Such statement could lead the legislator to heavily weigh the protection of privacy and fundamental rights in the legislation.

However, in a globalized world, innovation and economic wealth are relevant values and cannot be ignored. A strong economy has direct effects on the life standards of a society and, therefore, a country's wealth is paramount to guarantee that fundamental rights are respected.

Thus, the Charter provides the right of freedom to conduct business as a fundamental right in its article 16. That means that companies must be given some protection and flexibility on how their business is conducted. Such article gives economic rights some level of protection, even if indirectly[6]. Accordingly, recital 4 of the new Regulation clearly states that privacy and data protection are not fundamental rights and shall be balanced with other rights, including the right of freedom to conduct business.

Profiling and Online Behavioural Advertisement (OBA) are relevant part of the debate on protection of user's rights as opposed to the exploitation of economic interests. The use of data has been proven to be important for business, whereas it can seriously impact user's privacy. In this sense, the Regulation brings relevant provision on the treatment of profiling and behavioural advertisement, including: i) expanded definitions for personal data, including IP Address and cookies in the scope of the regulation; ii) stricter requirements for obtaining consent and; iii) definition and specific provisions for profiling.

---

[5] Proposal of the Commission COM(2012)0011. See also:
http://www.lexology.com/library/detail.aspx?g=981b312b-3c22-4631-b7d9-a390952efac1

[6] Freedom to conduct a business: exploring the dimensions of a fundamental right, © European Union Agency for Fundamental Rights, 2015. As explained in the Report, the freedom do conduct business has been playing an important role on the Europe 2020, which provides guidance of the economic development of the Union.

Yet, the final text of the Regulation has brought more flexibility for the industry engaged in behavioural profiling than the proposal of the Commission. For instance, legitimate interest of the data controller was found to be a legal basis for the processing of data to direct marketing[7] and profiling for direct marketing was given specific treatment, being separated from the article that regulates profiling when it produces legal effects or significantly affects data subjects.

Given the scenario above and considering the challenges of the legislators when approving the new Regulation, the purpose of this work is to analyse whether in regard to profiling for market purposes, the GDPR provides effective protection of privacy and data protection without undermining the economic potentials of the exploitation of a data-driven economy.

1.1 Legal Questions

Since the introduction of the proposal for Regulation by the Commission, the legislative process of the GDPR was surrounded by high pressure from privacy advocates and the industry, which has led to several amendments and changes in the final text of the Regulation

In comparison with the DPD, the Regulation brings several innovations. It provides citizens more rights and safeguards, whereas business will have additional obligations in terms of compliance. However, privacy advocates argue that theirs "initial grand ambition was not achieved", as the final text of the Regulation is substantially different (and less restricted) than the text of the proposal[8]. Meanwhile, the industry recognizes that, although the GDPR has brought challenges and new obligations, it has maintained some level of flexibility on the conduction of business[9].

Given these scenario, the legal questions to be answered in the work are:

1) Regarding profiling and online behavioural advertisement, has the GDPR substantially increased the level of protection of users in the digital environment, namely the right to privacy and data protection?

2) Has the GDPR maintained some level of flexibility to companies engaged on placing online behavioural advertisement within their right to conduct business and to explore the economic potential of a data-driven economy?

[7] Recital 47 of the Regulation

[8] https://www.privacyinternational.org/node/689

[9] https://www.helpnetsecurity.com/2016/05/25/gdpr-reactions/

Aiming to answer the questions above, this work shall encompass: i) an explanation on how profiling and online behavioural advertisement are placed in the digital context and; ii) an analysis on the potential effects of profiling and online behavioural advertisement within privacy and data protection. Regarding the relevant legal framework to deal with profiling and OBA, this work shall outline: iii) the fundamental rights at stake, namely privacy and data protection and the right to conducts business and; iv) the secondary legislation, i.e., the DPD, EPD and the Regulation. The comparison between the previous legislation within the new Regulation is the main focus of this work. Yet, this work provides: v) a comparison between the European legislation with the regulation of the US, as the latter plays an important role in the digital economy. The final sections of this work aims to answer the legal questions and provide conclusions.

1.2 Methodology

This work in conducted based on the study of legal instruments, namely International Treaties, European Union primary and secondary legislation, as Treaties, Convention, Directives and Regulations. The main instruments to be taken into consideration are the Treaty on the Functioning of European Union, Charter of Fundamental Rights of the European Union, the DPD, the EPD and the GDPR.

In addition to the analysis of legal instruments, case law and literature (books and journals) will be relevant sources on the research. Opinions of the Working Party 29 and other organizations and institutions engaged on the enforcement of privacy and data protection rights shall be considered. Such opinions shall be confronted by opinions and documents prepared by or under the supervision of the industry, as technology companies and marketing institutions and associations.

1.3 Definitions and Core Concepts

This work shall encompass some technical terms, given that it deals with relevant terminologies in the digital context. Therefore, some definitions might help the understanding of the following chapters. Thus, the following definitions shall be taken into consideration:

Online Behavioural Advertisement - is advertising that is based on the observation of the behaviour of individuals over time[10]. It means the tracking of a consumer's online activities

[10] Working Party 29 – Opinion 02/2010 on Online Behavioural Advertisement

over time, in order to deliver advertising targeted to the individual consumer's interests[11]. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests[12].

Profiling – The GDPR defines profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[13]. It can also be described as "a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from data in the form of constructing profiles that can subsequently be applied as a basis for decision-making[14].

Cookies – is a piece of text stored by a user's web browser and associated to a HTTP request[15]. It transmits information back to a website's server about the browsing activities of the computer user on the site[16]. Cookies are the most used and known tracking tool currently in place.

Ad Network Providers – distributor of behavioural advertising and responsible for connecting publishers with advertisers[17]. Ad network providers are companies that control targeting technologies and associated databases with the aim of distributing advertisements to publishers[18].

Big Data Analytics - can be understood as the process of examining large data sets to uncover hidden patterns, unknown correlations, market trends, costumer preferences or other useful information[19].

---

[11] FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising

[12] Ibid.

[13] Regulation, article 4

[14] Working paper on profile (V. Ferraris et all UNICRI) http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf

[15] Gutwirth, Serge et all, European Data Protection: In Good Healt,

[16] Supra at 11.

[17] Opinion 02/2010 – WP.

[18] Ibid.

[19] ttp://searchbusinessanalytics.techtarget.com/definition/big-data-analytics

2. WHY PROFILING AND ONLINE BEHAVIOURAL ADVERTISEMENT ARE A PRIVACY MATTER

In the current digital economy, data is a commodity, which means that actors who want to be competitive must participate in the "data race". The tech industry has, currently, advertisement as the main source of revenue. For instance, Facebook income in advertisement can reach billions of dollars per year[20], whereas Google is expected to have even higher revenues[21].

Processing data with the purpose of placing advertisement is important not only to the tech industry. Collection and analysis of data have been found to be very effective to companies on the studying of patterns and behavioural of theirs consumers. Consequently, it enables companies to improve products and services and to place more attractive advertisements.

The phenomenon called Big-Data, i.e., the existence of data sets extremely large and complex, within the emergence of new technologies capable to analyse and manage this massive amount of data, has opened a wide spectrum of possibilities, including business opportunities based on the study of data[22].

Thus, collection and processing of data became undoubtedly the most effective technique on conducting business in the digital economy. Accordingly, deployment of more effective methods of collection and management of data is rapidly increasing.

Even though consumers have the advantage of being offered with services free of charge and more attractive advertisement, most of internet users are not aware of the existence of a huge market in which their data are flowing and being commercialized in the online environment. While surfing in the Internet, users are generating massive amount of data, some of it personal data, which have been processed by different agents, many of them unknown to users.

[20] The Wall Street Journal http://www.wsj.com/articles/facebook-posts-strong-profit-and-revenue-growth-1469650289

[21] Ibid.

[22] Francesco Corea, Big Data Analytics: A Management Perspective, Springer, 2016, page 2

2.1. Tracking, Profiling and Online Advertisement

The process of collection of data with the purpose of analysing the behaviour of users and subsequently offering tailored advertisement is common referred as Online Behavioural Advertisement, Behavioural Profiling or Online Tracking.

Online advertisement can take place through observation of behaviour of people (behavioural advertisement) or through "snap shots" of what data subjects view or do while accessing a particular website[23]. For instance, contextual advertisement takes place in search engine as Google, when an advertisement matches the interest of the user according to the words that the user types in the search. Segmented advertisement is often used by social media as Facebook, when the agent process data submitted by the user when registering into the website.

Contextual advertisement is outside of the scope of this thesis, as it is not potentially harmful to privacy and data protection as advertisements based on the analysis of behaviour[24]. This work shall focus on the hypothesis in which agents can track users over a time and can collect data from different sources. Therefore, Google might engage in behavioural advertisement when it tracks consumer for a length of time. However, the cases in which the advertisement is placed based exclusively on a single search on Google, there is no collection of data over time. Thus, this type of advertisement is not covered in this work

The relevance of behavioural advertisement in the privacy and data protection relies on the cases in which profiles of users are built with the purpose of providing tailored advertisement. Such practice can be referred as profiling.

Hildebrant describes profiling as "the process of discovering correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category"[25].

Profiling can be useful in different contexts, namely law enforcement agencies, monitoring of employers, academic researches and for private companies to customize their services and

[23] Working Party 29, Opinion on online behavioural advertisement 02/2010

[24] According to the FTC Report on Online Behavioural Advertisement, this type of advertisement is not potentially harmfull. The Working Party 29, in the opinion on online behavioural advertisement equally did not treat this sort of advertisement..

[25] Hildebrant, Profiling the European Citizen, page 19

advertisement. This work shall encompass only profiling by private companies, with the purpose of offering tailored advertisement. Such type of profiling is possible due to the collection of data through several tracking technologies.

Regarding profiling in the business industry, Clarke explains that profiling is "used by corporations, particularly to identify consumers likely to be susceptible to offers of goods or services, but also staff-members and job-applicants relevant to vacant positions"[26] .

As pointed out in the Report of the Norwegian Data Protection Authority[27], nowadays profiles are built based on information collected through "individuals' browsing history, updates on social media, which news articles they read, products brought on the Internet and registered customer information". Accordingly, profiling is to a great extent using Big Data analysis to look for patterns and connections[28].

The building of such profiles and the placement of tailored advertisement involves a complex relationship between different stakeholders, many of them unknown by internet users. The stakeholders involved on the placement of behavioural advertisement are publishers, advertisers and ad network providers.

The publisher or website provider is the owner of a website that contains a space where an advertisement can be placed. A publisher can be a newspaper website, as BBC, an e-commerce platform as Amazon or a social media, as Facebook. More popular the publisher, higher the potential for placing advertisement, as advertiser will be more willing to pay for publishing in such platforms. Many websites can offer free services to the users due to the revenue it gets from advertisement.

The advertiser is the company who wants to place an advertisement in a website with the aim of offering its products and services. For instance, a sports company might want to advertise new products. Instead of placing ads for a range of people, this advertiser now is able to offer direct ads to users that are more likely to be interested in its products or services.

The most complex players involved on the placement of tailored advertisement are the agents engaged in buying and selling ad spaces. These agents are called ad network providers and

[26] Clarke R. (1993)

[27] The Great Data Race, How comercial utilisation of personal data challenges privacy. Report, November 2015; Datatilsynet

[28] Ibid.

they are engaged in connecting publishers to advertisers[29]. These ad network providers normally use a marketplace called ad exchange, where purchasers of ad spaces can place offers to buy ad space offered by the publishers[30].

Ad network providers may take different forms, as supply-side platforms (forms of software developed to sale on ad exchanges), demand-side platforms (types of software that serve ads on behalf of advertiser), data brokers (companies that collect consumers' personal data and resell or shat that information with others)[31].

In summary, the tailored advertisement is placed when a publisher reserves a visual space on its website and an ad network provider distributes such ad spaces to the purchase of advertisers. The purchase normally is made through a real-time bidding, which might involve different ad network providers and several publishers. Due to placement of advance software, all the process takes less than a second[32].

This whole process can be exemplified as follows: the user accesses BBCs website. BBC, taking the role of a publisher, reserves some space in its website to the placement of advertisement and it gets into negotiation with one or more ad network providers, who are responsible to offer these ad spaces to different advertisers. Given that ad network providers place tracking tools in user's web browsers, usually in the form of cookies, they are able to give advertisers information about the users that will access the advertisement. Thus, the ad network provider will deliver advertisers the characteristics of the user that is accessing BBC's website, for instance, a man, between 30-40 years old, who is used to travel and often visits sports websites. Advertisers can then send a bid. In this case, is more likely that travel agencies or sport clothes companies shall be interested in placing an advertisement of flight tickets or sports clothing and will give a higher bid. The bidder with the highest bid shows the ad in BBC website.

That means that more data the ad networks provide to the advertisers, better elements the advertiser has to choose ad spaces with the aim to place a tailored advertisement. Consequently, it is more likely that the users will click in the ad, which means, more revenue to the agents involved.

[29] Supra at 23
[30] Datatylsnet, ibid.
[31] Ibid.
[32] Ibid.

The scenario above evidences the importance of the collection of as much data as possible by the ad network providers.

The phase of collection of data can be referred as Behavioural Tracking[33]. Nowadays there are several different types of tracking methods designed to track consumers and to collect data in the online environment. It is likely that not all different technologies are referred in the literature, due to the dynamism of the sector.

The main example on the potential of collection of data and tracking is probably Google. Google is the biggest company in the technology segment, owner of several different platforms and the provider of a range of services as Gmail, Youtube, Google Maps, Street View, Data Analytical Solutions and others. Thus, Google has a huge potential on collection of data. Google Maps collects location data, while search engine and Youtube might collect information about interests of people and their browsing history, including what searches the users' have conducted. Meanwhile, Gmail collects data through the registration process, which may include name, phone number and address.. If all these data are combined, Google might create very accurate profiles.

Facebook has also a huge potential of profiling, as it collects all sort of information about users' interest. Facebook has been under investigation about some of its tracking tools, for instance, collection of data through the like button, even when users are visiting other website without being logged in the social media[34]. Data analytics also have a huge potential on the collection of data within Big Data and the Internet of Things.

Nonetheless, the main tracking technology currently used by the agents engaged on placement behavioural advertisement is cookies.

2.1.1. Cookies

A cookie is a "piece of text stored by a user's web browser and associated to a HTTP request"[35]. It consists of "one or more name-value pairs containing bits of information and is set by a web server"[36].

---

[33] Claude Castellucia, Behavioural Tracking on the Internet: A Technical Perspective, from European Data Protection: In Good Health?; Springer, 2012

[34] https://www.grahamcluley.com/facebook-using-ads-track-including-non-users/

[35] Datatilsynet, The Great Data Race – How comercial utilisation of personal data challenges privacy. Report, November 2015

[36] European Data Protection: In good health; Serge Gutwith et all; Springer, 2012

Cookies allow companies to track users as it records the user's browsing activity. It can be first-party cookies (placed and controlled by the website owner) or third party cookies, which are controlled by companies other than the website owner. Third-party cookies allow the record of user's browsing activity on different websites and are potentially more harmful to privacy, as it can allow companies to build profiles based on information about a range of websites visited by the user. Studies show an increasing presence and tracking of third-party sites used for advertising and analytics[37].

The easy methods of circumventing the placement of cookies has made the industry to develop more sophisticated types of cookies, as evercookies and supercookies.

2.1.2. Supercookies and Evercookies

Due to the existence of known techniques to avoid tracking cookies, the industry has developed more robust tracking mechanisms[38], for instance the called supercookies. Supercookies can be stored outside the browser's control, which do not allow users to control them[39]. Persistence of Supercookies can be further improved as illustrated recent evercookies[40], which identify a client even when other types of cookies are removed. Some Supercookies and Evercookies do not expire and, therefore, this sort of cookies can be more intrusive in terms of privacy

2.1.3. Web beacons

Web beacons might also be an effective tracking tool. It usually consists in invisible graphic image placed on the website. It might be used by third parties to collect information about users or as a mechanism for placing cookies. It can be used on its own or in combination with cookies[41].

The placement of such technologies can trace consumers towards the collection of browsing history and other important means of identifying online users, as IP address and device fingerprinting.

---

[37] Krishnamurthy and Willis 2009b, 2009c

[38] Serge Gutwith, supra at 26.

[39] Ibid.

[40] Ibid.

[41] Supra at 35.

IP Address

IP addresses are identifiers related to a unit (PC, table or smartphone) that is connected to the Internet. It is the ID of the user while he is surfing in the Internet and, therefore, it can be linked to a person. IP can be static (an address permanently assigned to an user by the ISP) or dynamic (address dynamically assigned by the ISP, i.e., every time the computer or router is initiate, it assigns a different address). Static IP was considered as personal data on the Scarlet Case[42], whereas dynamic IP was recently found as personal data in the Patrick Breyer v. Bundesrepublik Deutschland case[43].

Device fingerprints

Device fingerprints are information collected about a computer, or the unique electronic fingerprint that every computer has when it is connected to the Internet. It was found that web-based device fingerprinting might collect enough information about a user even when cookies are not placed[44].

2.2. Main Legal Implications of Profiling

As evidenced above, personal data has been collected, analysed and used on a daily basis, insofar as the users are not aware of such practices or who are the agents involved. As affirmed by Nancy King "Most people do not know they are being tracked, and they aren't given a choice whether to be tracked or to have their online behaviour and personal information shared with large networks of advertisers".

The debate about the legality of profiling and the extent of such legality must consider, on the one hand, privacy and data protection as a fundamental rights, and, on the other hand, the market opportunities, the freedom that companies have to operate theirs business and the economic and innovative benefits that might be brought in the digital economy.

For instance, tailored advertisement can support the offer of free services and can bring more specific advertisements to consumers according to their preferences, in what is said to be a benefit for the society. Moreover, there is huge economic potential in the usage of data by the

[42] ECJ, Case C-70/10Scarlet v Sabam November 24, 2011

[43] ECJ, Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland, October 19, 2016

[44] http://motherboard.vice.com/blog/device-fingerprinting-can-track-you-without-cookies-your-knowledge-or-consent

industry. Studies reveal that Big Data and open data may increase, for instance, the GDP of the UK in 2.9% and economy-wide benefits could raise EU-28 GDP by 1.9% by 2020[45].

However, it is undeniable that companies involved in digital marketing entails the use of highly intrusive mechanisms in the extraction, analysis and use of personal data when creating a profile and targeting advertisements. The extent of the impacts on the individual is difficult to assess.

Profiling has consequences on the individuals and the society. Such risks might involve discrimination, inequality, stereotyping, stigmatization and inaccuracy of the decision-making process[46]. According to Hildebrant[47], growing relevance of profiling technologies, among the general evolution of digital technologies, makes society face the risk of dependence and unable to control the process and the effects of those technologies. For instance, Shoshanna Zubbof introduces the idea of a surveillance capitalism, where "subjugation are produced as this innovative institutional logic thrives on unexpected and illegible mechanisms of extraction and control that exile persons from their own behaviour"[48]. According to Zubbof, "democracy no longer functions as a means to prosperity; democracy threatens surveillance revenues"[49].

Undoubtedly the impact on massive collection of data and its potential to discriminate a person or a group of person raises legitimate concerns. However, it is important to understand to what the extent such concerns are related to privacy and data protection, and to which extent other legislations shall apply, for instance, anti-discriminatory rules and competition law. Moreover, it is paramount to differentiate the cases in which data processing is intrusive and illegal to the cases in which processing of data is potentially beneficial to innovation and not harmful in terms of privacy. For instance, placement of a tailored advertisement based on browsing history does not have the same effect on users as the raising of insurance value based on the analysis of consumer behaviour in the Internet. Although both cases can be based on profiling, the legal effects are substantially different.

[45] Stéphane CIRIANI, The Economic Impacts of the European Reform of Data Protection, Communications & Strategies, 2015, Issue 97, p.41(18)

[46] Profiling and impacts in individual rights

[47] Hildebrandt, 2009c

[48] Zubboff 2015

[49] Zubboff 2015

Specialists might say that behavioural advertisement is the tip of the iceberg[50], as it is the starting point of the massive collection of data, which in a higher extent can lead to control of behaviour of people and a surveillance capitalism. Indeed, the massive collection of data raises questions on how behaviour of people and the access of information can be manipulated towards the manipulation of data.

However, preventing a legitimate practice under the assumption that it leads to further illegal acts is not the best legal approach. The law has to deal with each legal situation individually. Therefore, Google might place advertisement based on behavioural profiling legally, but it can breach the law in cases of abuse of power due to the massive collection of data. Both situations are different and must be handled accordingly.

Therefore, it is important to establish the boundaries of the legal implications of online behavioural advertisement within the legal implications of other practices based on collection of data for other purposes. Behavioural advertisement is relevant for privacy and data protection, but not to the same extent as profiling for discriminatory purposes, this latter not being in the scope of this work.

3. LEGAL FRAMEWORK ON PROFILING AND OBA

3.1 Privacy and Data Protection as a Fundamental Right

After the World War II, several international conventions on human rights were adopted, including the Universal Declaration of Human Rights[51] and the International Covenant on Civil and Political Rights[52], which expressly recognized the protection of privacy and data protection.

Since 1953, when the European Union adopted the European Convention of Human Rights, citizens are guaranteed the right to private life and non-interference of theirs private communications.

---

[50]Zuiderveen Borgesius, Frederik, Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, April 2016, Vol.32(2), pp.256-271

[51] Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[52] Article 17: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

After the signature of the Treaty of Lisbon, privacy and data protection became fundamental rights in the European Level. Article 16 of TFEU and articles 7 and 8 of the Charter of Fundamental Rights gave the European Union a mandate to ensure data protection and laid down the tasks of the Union in relation to privacy and data protection[53]. The protection of privacy and data protection are equally established in other International treaties, as the Convention 108[54], which firstly introduced the right to not be subject to automated decision, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Under European Union Law, privacy and data protection are "distinct, yet complementary, fundamental legal rights", as they "derive their normative force from values that—although at times coincidental and interacting in a variety of ways—may be conceptualized independently[55]".

The right to privacy, as laid down in article 8 of the ECHR and article 7 of the Charter, provides the citizens the right to "be left alone" and to have secrecy over their communications. It is commonly referred to the right of not being subject to arbitrary interference from public authorities[56].

In relation to data protection, it has an individual legal treatment on the Charter and other instruments. Data protection as a fundamental right has "allowed data protection to automatically trump other interests and gives it a status that cannot be traded-off for economic benefits.15[57]". As such, data protection assure data subjects the right of being informed about what is done with their data and to not have their data processed without legitimate purposes or consent.

[53] Hijmans, Hielke; The European Union as Guardian of Internet Privacy, The Story of Art 16 TFEU, Springer, Law, Governance and Technology Series, Vol. 31, 2016, page 4

[54] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

[55] Maurizio Borghi, Federico Ferretti, and Stavroula Karapapa, 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK' (2013 Vol. 21 No. 2) International Journal of Law and Information Technology 109–153

[56] Bygrave A Lee; Data Protection Pursuant to the Right to Privacy in Human Rights Treaties; International Journal of Law and Information Technology, 1998, volume 6, pp. 247–284

[57] Supra 53

As fundamental rights, privacy and data protection are essential values in democratic societies and are subject to the rule of law[58]. However, such rights are not absolute and must be balanced with the other fundamental rights, as freedom of expression, property and, more important to this work, the right to conduct business. Such balance must be taken according to the principle of proportionality, as stems from article 52 (1) of the TFEU.

For instance, national security might override the right to privacy in cases of national security. Freedom of expression is often capable of limiting the right to privacy, for example, in cases involving celebrities. As public people, celebrities are more subject to interference to their rights, as aspects of their life gives rise to interest from other people. Thus, right of privacy must be balanced with freedom of expression and journalism.

Given that online behavioural advertisement often leads to processing of personal data, it may have implications on fundamental rights. The Charter provides that processing of personal data must be carried out within a legal basis, as consent or legitimate interest of the data controller. Failure to comply with such rules might give rise to violation of fundamental rights as laid down in the Charter.

3.2. Right to Conduct Business as a Fundamental Right

Stakeholders engaged on the placement of online behavioural advertisement often justify their activities on economic causes, as the need of increasing innovation and taking advantage of data exploitation to foster economy. Indeed, online advertising is a key source of revenue for several online services as it influences the growth of internet economy and it supports a range of services that are offered free of charge[59].

However, innovation and potential economic benefits are not expressed referred as fundamental rights, despite its relevance in a globalized society. However, despite the fact that the Charter does not contain provisions relying on economic interests, it establishes the freedom to conduct business as fundamental rights, as stemming from article 16. The right to conduct business has equally become a fundamental right after the signature of the Lisbon Treaty.

---

[58] Supra at 53

[59] About economic importance of data in the business: Mc Afee and Brynjolfsson: the more companies characterised themselves as data-driven, the better they performed on objective measures of financial and operational results… companies in the top third of theirs industry in the use of data-driven decision-making were, on average, 5% more productive and 6% more lucrative than their competitors .

The essence of the right to conduct a business is to promote entrepreneurship and innovation, which are "indispensable for sustainable social and economic development"[60]. Such right has being used "more forcefully to balance other rights and underpin proportionality testes of various intrusive measures[61]".

The right to conduct business was found to be relevant in a range of EU policies related to the Single Market, economic growth and entrepreneurship. It is directly linked to economic growth, particularly in the EU's growth strategy "Europe 2020" objectives, namely employment, innovation and social inclusion[62].

Therefore, companies engaged on the placement of online behavioural advertisement do have a fundamental right to rely on, as their activities are relevant on fostering European Union's economy. Nonetheless, the right to conduct of business is not an absolute right and is subject to be overridden by other fundamental rights.

The right to conduct business was already referred as a weak right[63], as it is more subject to the interference of other rights. Particularly in Europe, where citizens are guaranteed a highly level of protection of its rights, the free initiative finds more obstacles on the conduction of business.

Accordingly, cases involving the right to conduct business and its interference within other rights are often ruled based on the principle of proportionality and grounds as equality, legitimate expectations and fundamental freedoms.

For instance, in the case Sky Osterreich GmbH[64], the ECJ has stated that "..on the basis of that case-law and in the light of the wording of Article 16 of the Charter (…) the freedom to conduct a business may be subject to a broad range of interventions on the part of public authorities which may limit the exercise of economic activity in the public interest" .

---

[60] Freedom to conduct a business: exploring the dimensions of a fundamental right; European Agency for Fundamental Rights, 2015

[61] Ibid.

[62] Ibid.

[63] Groussot, Xavier and Petursson, Gunnar Thor and Pierce, Justin, Weak Right, Strong Court - The Freedom to Conduct Business and the EU Charter of Fundamental Rights (April 23, 2014). Lund University Legal Research Paper Series No 01/2014. Available at SSRN: https://ssrn.com/abstract=2428181 or http://dx.doi.org/10.2139/ssrn.2428181

[64] Case C-283/11 Sky Österreich

Nonetheless, the right to conduct business has already been important in judgments of the ECJ. For instance, in the cases Scarlet[65] and Netlog[66], the ECJ had to strike a balance between the rights of copyright owner (IP Law) with the right to conduct business. In the final ruling, the Court understood that the obligation of an ISP to install a filter aiming to analyse the content of electronic communications and therefore avoid proliferation of material protected by copyright, would not be reasonable considering the right of conducts business, as it would impose an unfair burden on the ISP.

Thus, it is important to take into consideration that there is a limitation on the interference of business operation. Even though there is not mention of innovation and economic interests as fundamental rights, the right to conduct business might be relevant on the defence of business interest and it is intrinsically related to European's economic growth.

Regarding the legal implications of profiling in the new Regulation, some of the obligations imposed by the GDPR demands an assessment on whether privacy might be overridden by other interests, which may include the right to conduct business. For instance, over restriction on the use of some tracking technologies might disrupt some business activities. In such cases, a proportionality approach must be taken, aiming to evaluate in which extent the data protection might overridden the right of a company to carry out commercial activity.

In such analysis, economic aspects must be considered, as innovation and economic wealthy are relevant values in democratic societies.

3.3. Secondary Legislation

Under European Union Law, the main regulatory instrument to safeguard the right to privacy and data protection is the Data Protection Directive (Directive 95/46/EC or DPD). The Directive is dated from 1995, when the Internet was still in development. Therefore, the DPD was not designed to deal with the advanced technologies currently in place.

The deployment of new technologies in the online environment has led to the issuance of the Directive 2002/58/EC, so-called ePrivacy Directive (EPD), which aimed to protect privacy in electronic communications sector. The EPD was adopted in 2002 and later amended by the Directive 2009/136/EC. The EPD has brought an important provision regarding the processing data in the digital context. Article 5 (3) of the EPD, so-called the cookie provision,

[65] Case C-70/10: 'Scarlet Extended v, SABAM

[66] SABAM v. Netlog (CJEU C 360/10)

has regulated information stored in terminal equipment, which applies to the placement of cookies[67].

Although the applicability of the ePrivacy Directive in principle would prevent the applicability of the DPD (lex specialis derogat legi generali), Recital 10 of the EPD establishes the applicability of the DPD 'to all matters concerning protection of fundamental rights and freedoms which are not specifically covered" by the EPD.

Therefore, both Directives are applicable to data controllers engaged in behavioural advertisement. While the EPD contains rules on the processing of data through electronic communications, in particular to the placement of cookies, DPD shall apply when behavioural advertisement entails the processing of personal data. The Article 29 Working Party has already reinforced the full applicability of the DPD, with the exception of the provisions that are specifically addressed in the E-Privacy Directive[68].

3.3.1. Applicability of the ePrivacy Directive to Online Advertisement

As explained in section 2.1.1., cookies are found to be the main tracking tool currently in use by the agents involved in online behavioural advertisement. Through the placement of cookies agents can track browsing history and collect substantial information about users. Considering its potential effects on privacy and data protection, the EPD has introduced the so-called Cookie Provision, laid down in article 5 (3) of the Directive 2002/58/EC, as amended by the Directive 2009/136/EC.

Article 5(3) of the EPD, combined with recital 24, establishes that information stored in a terminal equipment relates to private information and, therefore, storing information or gaining access to information stored in the terminal equipment of subscribers' demand consent from the user. As explained by the Working Party 29, tracking cookies are information stored in users' terminal equipment and they are accessed by ad networks when data subjects visit websites related to the ad network[69]. Therefore, online behavioural advertisement based on the use of cookies triggers the obligation to comply with article 5 (3) of the EPD. In the Opinion 9/2014[70], the Working Party 29 has stated the EPD applies to device fingerprint at the same extent it applies to cookies.

[67] Article 5(3) of the Directive 2002/58/EC as amended by the Directive 2009/136/EC

[68] Supra at 23

[69] Supra at 23

[70] Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting

It is important to note that such article does not refer to personal data, but to any information stored in the terminal equipment. Thus, it is not necessary that the information is classified as personal data to invoke the applicability of article 5 (3)[71]. The Working Party reinforces such statement in its opinion on behavioural advertisement[72].

Under the Directive 2002/58/EC, before the amendments of the Directive 2009/136/EC, placement of cookies and access to information stored in it should be allowed on condition that users were provided with clear and precise information about the purposes of the cookies and were given the opportunity to refuse to have cookies or similar devices placed (opt-out regime). The main change introduced by the Directive 2009/136/EC was the adoption of an opt-in regime. The amended version of article 5 (3), combined with recital 66 of Directive 2009/136/EC, requires consent and clear and comprehensive information, according to DPD, to the storage of information or gain of access to information stored in terminal equipment of a user.

The changes brought by the Directive 2009/136/EC have been criticized by stakeholders that argued that the opt-in regime raises costs and reduces revenue available to develop new online contents and services to consumers[73]. However, the opt-in regime of the amended version was softened in recital 66, which established that consent may be expressed by using the appropriate settings of a browser or other application when "it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC"[74].

The Working Party has raised concerns over consent be obtained through browsing settings and has stated that browser settings designed to accept all cookies would not deliver informed consent[75]. However, the lack of sufficient definitions in article 5 (3) combined with recital 66 leads to the conclusion that EPD is not clear enough in addressing requirements for obtainment of consent and arguably "failed to clear up the confusion over implicit consent with respect to browser settings[76]"

[71] . Damian Clifford, EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour 5 (2014) JIPITEC 194, , page 198)

[72] Supra at 23

[73] Daniel Castro and Alan Mcquinn, The Economic Costs of the European Union's Cookie Notification Policy, the Information Technology and Innovation Foundation, 2014

[74] Recital 66, Directive 2009/136/EC

[75] Opinion 02/2010, supra at 243

[76] Matthew S. Kirsch, Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising, 18 Rich. J.L. & Tech. 1. 2011-2012

Although the Working Party has recommended the adoption of an opt-in regime, a survey conducted by the Working Party has showed that, in a range of 478 e-commerce, media and public sector websites, more than half does not require consent to the placement of cookies, but provide a banner informing that cookies are in use[77] and therefore rely on an opt-out regime.

The result of the survey conducted by the WP 29 evidences that the cookie provision is not an effective rule. According to Lokke Morel, the Amended version of the EPD, when providing an opt-in regime to all types of cookie and by giving the users to many rights, has made the cookie rules ineffective[78]. She has argued that the EPD has failed when it gave equally treatment for all types of cookies, whereas if it has offered different treatment for each type of cookies, the legislation would be more effective[79].

It is important to note that the EPD is not derogated by the new Regulation. Nevertheless, the EPD shall be revised, aiming to be harmonized with the GDPR.

3.3.2. Applicability of the DPD to Online Behavioural Advertisement

As laid down in recital 10 of the Directive 2002/58/EC, the EPD directive does not prevent the applicability of the DPD, as the latter applies to "all matters concerning protection of fundamental rights and freedoms" not covered by the EPD. Nonetheless, online behavioural advertisement may be placed towards the use of technologies other than cookies and that are outside the scope of EPD.

Online behavioural advertising falls within the DPD when personal data (information about an identified or identifiable person[80]) is processed by the data controller. Processing within the DPD means any operation or set of operations performed upon personal data[81].

Definition of personal data in the digital context can be challenging, as the Internet has brought forms of interactions in which users' devices can be identified, when the real person cannot. The regulation provides that an identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more

---

[77] Cookie Sweep Combined Analysis – Report (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf)

[78] Moerel, E. M. L. (2014). Big data protection. Tilburg: Tilburg University.

[79] Moerel, E. M. L. (2014). Big data protection. Tilburg: Tilburg University.

[80] Article 2 (a) of the DPD

[81] Article 2 (b) of the DPD

factors specific to his physical, physiological, mental, economic, cultural or social identity"[82]. The ECJ has already decided that a person can be identified by other means than name, including telephone number, information about hobbies or working conditions[83]„

Whether information processed in the context of providing online behavioural advertisement falls within the scope of the Directive is debatable.

The Interactive Advertising Bureau states the online behavioural advertisement does not fall within the DPD, as the information collected is not personal, once it does not identify a real person and no personal information, such as name, address or email address is processed[84]. The Working Party opinion on behavioural advertisement refuses such argument, on the basis that "names are not always a necessary means of identifying individuals". The WP states that targeted marketing clearly falls within the scope of the Directive as cookies can involve the processing of unique identifiers and the collection of IP Addresses. Furthermore, the information that is collected relates to the users' characteristics, and this is used to influence their behaviour[85]. Moreover, the creation of profiling may include a pattern of online behaviour, which the uniqueness can link to an identifiable person. Thus, if a company uses data to "single out" an individual, or to distinguish an individual within a group, personal data is being processed[86].

Considering that the ECJ has already decided that IP Addresses are personal data and cookies often entail the processing of personal data, it seems rather difficult to argue that online behavioural advertisement does not fall within the scope of the Directive. Furthermore, the new Regulation expressly recognizes IP Addresses and cookies as personal.

Who is the data controller and who is subjected to the applicability of the rules

As explained in the section 2.1, online behavioural advertisement involves different agents, namely the publisher, the advertiser and ad network providers.

[82] Article 2 (a) DPD

[83] Case Lindqvist, 101/01

[84] Interactive Advertising Bureau. Your Online Choices. A Guide to Online Behavioural Advertisement (www.youronlinechoices.com/uk/about-behavioural-advertising)

[85] Opinion 2/2010 on online behavioural advertising

[86] Frederik J. Zuiderveen Borgesius, Personal data processing for behavioural targeting: which legal basis? International Data Privacy law, 2015

The most popular and privacy intrusive tracking tool is third party cookies, which are placed by ad networks. Ad networks collect information about users and trace the browsing behaviour of consumers with the aim of providing detailed profiles to potential advertiser. Among the data collected by ad networks are IP Addresses and other technical information that might be able to individualize a user. Therefore, it seems clear that ad networks will fall within the definition of data controller as laid down in the DPD[87], as it collect and process the information and place and design the cookies used to retrieve the information[88].

Assessing whether publishers are data controllers is rather complicated, as it does not process data itself, but may facilitate the collection of data instead.

According to the Working Party 29 publishers can be joint-controllers in some situations, for instance, when the publisher sets up its website in such a way that a visitor of a publisher website is redirected to the ad network website. In such situations, the user would be redirected to the website of the ad network, in which his IP would be collected. However, the IP would not be collected if the publisher's website was designed in a different form.

In this case, the WP 29 states that although the publisher does not transmit the IP Address, it allows the ad network to collect the IP address and to place cookies. Thus, the WP argues that the publishers triggers the transfer of IP Addresses and contribute with the tailored advertisement in this specific situation. Notwithstanding, the WP imposes limits on the liability of the publisher, stating, for instance, that such responsibility cannot require compliance with the bulk of the obligations contained in the Directives[89].

Although the interpretation of the WP seems to be over restricted, the ECJ appears to give data controller a broad interpretation, as stemming from the decision related to the right to be forgotten[90]. Therefore, publishers might need to take some precautions on the way they design theirs websites, under the consequence of being found as a joint-controller.

.

As for the advertisers, the WP states that it will be a data controller only when it captures the targeting information and combines it with onsite surfing behaviour[91].

---

[87] article 2 of the DPD, "controller" is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'

[88] Supra at 73 pag. 198

[89] Supra at 23.

[90] Google Spain v AEPD and Mario Costeja González, C 131/12 of the ECJ

[91] Supra at 23

Main principles and obligations under the DPD

According to article 8 of the Charter, personal data might be processed when the controller has a legal basis for the processing. Such legal bases are listed in article 7 of the DPD.

The main legal basis for the processing of personal on the context of behavioural advertisement is consent. There is a heat debate on whether consent on the placement of cookies, according to article 5 (3) of the EPD, means consent to the processing of personal data within the meaning of the DPD. The Working Party and some scholarships argue that consent under the cookie rule is different from the consent to the processing of personal data under the DPD. The main reason for such conclusion would be that the cookie rule has a different scope, i.e., it deals with information different from personal data and that the EPD provides subsidiary applicability of the DPD on the protection of fundamental rights.

Therefore, placement of cookie and processing of personal data obtained through the use of cookies would demand different consent, although it could be obtained concomitantly. Consent within the meaning of DPD, requires freely given, specific and informed indication of wishes, by which the data subjects signifies agreement to the processing of his data[92]. Such consent might be given in any form, including implicitly.

The two other legal bases for the processing of personal data under the DPD are necessity to perform a contract and legitimate interest of the data controller.

Considering that particularly regarding marketing practices the GDPR has been bringing substantial changes to the Directive, such legal basis shall be discussed in the next chapter.

3.4 The General Data Protection Regulation

The proposal of a General Data Protection Regulation in the European Union was introduced by the European Commission in January 2012, with the purpose of strengthening protection for individuals, particularly in the digital context. The Regulation aims to replace the DPD, unifying the regulation over the European Union and eliminating the inconsistencies over the national laws.

The GDPR has gone through a long legislative process, which has taken close to five years to be concluded. It is said to be the most lobbied legislation proposal in the history of EU, being

[92] Supra at 86

subject to around 4000 amendments on the Parliament[93]. The final text was approved on 27 April 2016 and the Regulation shall come into force on 25 May 2018.

The complexity of the legislative process evidences the challenge of regulating data protection in the digital environment, where strong privacy rules are rarely compatible with economic interests. Indeed, the GDPR offers a more comprehensive framework to deal with problems of the digital economy, as it better describes some of the digital technologies and provides better safeguards on the processing of data by online data controllers.

3.4.1. Principles

Under the DPD, the main principles on the processing of personal data are lawfulness, fairness, purpose limitation, data minimisation, integrity and confidentiality. In comparison with the DPD, the GDPR has brought two new principles, namely transparency[94] and accountability[95].

Although the regulation has not brought substantial changes on the principles as laid down in the DPD, it brought important obligation to data controllers, that are now obliged to process data in a transparent manner and to be able to demonstrate compliance with the Data Protection Principles. Furthermore, article 5 (1) (c) has strengthened the data minimisation principle, stating that personal data must be adequate, relevant and limited to what is necessary.

3.4.2 – Definition of Personal Data

The definition of personal data under the upcoming regulation sets out a more detailed wording to deal with the digital economy. Article 4 (1) combined with recital number 30, clarifies that natural persons may be associated with online identifiers provided by devices, "such as IP Addresses, cookie identifiers or other identifiers as radio frequency identification tages". Therefore, if a person can be identified through this means, the processing falls within the scope of the Regulation.

The introductions of the Regulation are aligned with the case-law of the ECJ, particularly regarding to the inclusion of IP Addresses as personal data, and with the Working Party

[93] Paul e Hert and Vagelis Papakonstantinou, The new General Data Protection Regulation: Still a sound system for the protection of inviduals., Computer Law & Security Review 32 (2016) 179-194

[94] Article 5 (1) (a) and Recital 39

[95] Article 5 (2) and Recital 85

opinions, that have already stated that cookie identifiers should be deemed as personal data. It also eliminates uncertainties in relation to the definition of personal data only when data were linked directly to a real person, as previous defended by some business stakeholders.

Pseudonymous and Anonymous Data

The legal treatment of pseudonymous data has raised intense debates. For instance, the industry representatives strongly called for soft or no rules for pseudonymous data, as it is not linkable to an identifiable person. Accordingly, regulating pseudonymous data and requiring consent for the processing of this type of data could discourage the industry to use pseudonymous data[96]. On the other hand, privacy advocates raised concerns on the possibility of advanced technologies being able to attribute pseudonymous data to an identifiable person.

The final text of the Regulation has included a definition of pseudonymisation in article 4 (3b), as the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person". According to recital 26, pseudonymous data might be found as information on an identifiable person whether attributed to a natural person by the use of additional information. Therefore, pseudonymous data might fall within the scope of the Regulation, although it does not provide much detail on the treatment of such sort of data.

As laid down in recital 28, application of pseudonymisation can reduce the risks to the data subjects concerned and help controllers and processors to meet theirs data-protection obligations. Therefore, although the Regulation does not provide detailed provisions on the processing of pseudonymous data, such practice is clearly encouraged, including when assessing data protection risk management.

As for anonymous data, it is not in the scope of Regulation, as explicit recognized in recital 26.[97]Such exclusion has raised some concerns for privacy advocates, that argue the anonymous data can be used in combination with other data to re-identify data. Some commentators even defend that the act of making a personal data anonymous entails the processing of personal data and, therefore, it would require consent from users.

[96] European Payment Institutions Federation (EPIF), EPIF's position paper on the General Data Protection Regulation, 2015, page 3

[97] Recital 26

Nonetheless, the exclusion of anonymous data from the regulation might encourage anonymization and underpin privacy concerns.

3.4.3. Consent

Consent has always been a core basis for legally processing personal data, as laid down in the Charter of Fundamental Rights. It has traditionally played a prominent part of European approach to privacy and data protection[98], as it relates to the autonomy of individual about the permissibility to the usage of personal data. According to the WP, "*consent is related to the concept to informational self-determination. The autonomy of the data subject is both a pre-condition and a consequence of consent: it gives the data subject influence over the processing of data*[99]".

The DPD defines consent as any "freely given specific and informed indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed". Article 7 further establishes that consent for the purposes of the Directive must be unambiguous. In summary, consent to be valid under the Directive has to satisfy the following criteria: being specific, informed, freely given, and unambiguously indicated.[100]

The main challenge of the Regulation is to turn consent meaningful in the digital context. Although the Directive sets out substantial requirements for the obtainment of consent, possibility of consent being obtained through setting browsing or through acceptance of terms and conditions has led to few consumers being able to give informed consent.

In comparison with the previous Directive, consent requirements have been strengthened in the Regulation. The Regulation now clearly states that an affirmative and positive action of the user is needed for consent is being valid[101]. Moreover, it establishes that pre-ticked boxes or inactivity do not constitute consent, but ticking a box or choosing technical settings of information society services, when it clearly indicates the acceptance of the users, can establish consent[102]. Consent under the Regulation shall be obtained for each different purpose and users shall be informed about how and for what purpose the data will be used. Users shall also be able to easily withdrawn consent.

---

[98] Eoin Carolan, The continuing problems with online consent under the EU's emerging data protection principles, Computer Law & Security Review 21 (2016) 462-473

[99] Opinion 15/2011 on the definition of consent

[100] Eoin Carolan, supra at 98.

[101] Recital 32 of the Directive

[102] Recital 32

An important provision on the consent requirement is that controllers shall be able to prove compliance with the rules of the Regulation, including obtainment of valid consent. Therefore, the controllers have the burden of proving that consent was obtained by legal means.

Undoubtedly, the new regulation provides a clearer and stronger meaning to consent. At least it attempts to guarantee some level of self-determination to the users, conferring upon them a greater leeway to decide when they want to share their data and for what purposes. Moreover, it aims to "eliminate the enforceability of implied consent through default settings by requiring an express indication of consent by the user."[103]

Even though it is clear that the Regulation has strengthened the requirements for obtainment of consent, the emphasis of regulators to rely on consent as the main legal basis for processing data in the digital context is often subject to criticism and scepticism[104]. For instance, the cookie provision on the EPD has already evidenced that strengthening consent's requirements not necessarily leads to obtainment of meaningful consent.

A main reason to question the consent approach is that decision-making in the online context is often "as much a matter of largely intuitive responses to particular prompts as it is a process of reasoned or deliberative reflection". According to Koops, in private and commercial contexts, consent is largely theoretical and has not "practical meaning", as it "denies the reality of 21st century data processing"[105]. Therefore, "convenience and people's limited capacity to make rational decisions prevent people from seriously spending time and intellectual effort on reading the privacy statements of every website, app, or service they use (…) There simply is no way in which ticking a consent box can 'ensur[e] that individuals are aware that they give their consent to the processing of personal data' in any meaningful understanding of 'awareness' of data processing practices and conditions".

Indeed, users often don't read terms and conditions or banners that pop-up in the browser. The easiness of eliminating banner through the option of clicking "I agree" often leads to 'individuals explicitly consent to agreements to execute clickwrap agreements and enduser

[103] Supra at 73

[104] Lokke Morel, Koops, Eoin.

[105] B.J. Koops (2014), 'The trouble with European data protection law',
International Data Privacy Law, doi: 10.1093/idpl/ipu023

license agreements (EULAs), and download apps granting whatever permissions are asked of them.'[106],

Under the rules of the GDPR, the user shall be granted more information, easy reading information and they have to act in an affirmative way to give consent. The new rules will have significant impact on the way agents place information online and require consent from the users. For instance, companies will have to offer the consumers a table of content containing the different purposes they want to process data for and give the consumers the opportunity of tick the boxes they want. Otherwise, agents can place different banners, each to require consent for each different purpose they want to process data. One of the concerns of industry representatives is that such requirements will make surfing in the Internet more annoying, as the consumers must deal with a range of new information.

Nonetheless, the capacity of the industry to innovate and to be able to obtain consent through new forms shall not be underestimated. Given the importance of processing data for many companies, the industry shall invest a lot of money on studies and development of more interactive forms to communicate with consumers, i.e., using of creative forms to persuade consumers to tick the box.

Based on the power of the industry and its engagement on finding such solutions, commentators have argued that "EU law's commitment to user consent as a core element of its data protection rules is neither neutral nor particularly pro-privacy. Rather, by assuming the empirical reliability of consent, the law is more likely in fact to facilitate rather than restrict the activities of data processors online[107]". Therefore, arguably "even the more robust model of active consent contained in the Parliament's draft could be deemed as ill-equipped, in practice, to secure the apparent objective of genuine consent in an online environment"[108].

Thus, a range of scholarships question consent as a legal basis for processing personal data in the digital context. Some commentators argue that any the approach based on consent would be incomplete or misconceived and even the most rigorous law would still not be sufficient signify presence of genuine user consent.

The proposal of the Commission included a provision that would strengthen the meaning of consent, namely a statement that consent should not be found as a legal basis for processing

[106] Omer Tene and Christopher Wolf, 'Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent' (Summer 2013 Vol. 4 Issue 3) Information Security & Privacy News19-28

[107] Supra at 98

[108] Ibid.

within a situation in which an imbalance between the data subject and the data controller would be found[109]. However, such provision was not subsumed in the final text of the Regulation.

Despite the critics on the emphasis of the regulation on consent, the GDPR seems to bring sufficient safeguards to users, as it gives much more obligations to the data controllers on the processing of personal data. It is likely that more rigorous provisions than the ones absorbed in the final text, if possible, would mean a few or zero flexibility to companies engaged on some type of activities.

3.4.4. Direct Marketing as Legitimate Interest of the Data Controller

Legitimate interest of the data controller is an independent legal basis for the processing of personal data. As explained by the WP, it has "its own natural field of relevant and it can play a very useful role as a ground for lawful processing[110]".

The GDPR has brought a relevant innovation on the legitimate interest of the data controller, namely a provision stating that direct marketing can be found as a legitimate interest of the controller, provided that it does not override the fundamental rights of privacy and data protection[111].

The Working Party's opinion 6/2014 has already acknowledged that legitimate interest under the DPD could be found as legitimate interest in some hypothesis. It provides some guidance on the conduction oh the balancing test, which shall consider the intrusion and impact the processing entails and the safeguards put in place by the data controllers and the mechanisms to object to the processing.

Accordingly, the WP opinion implies that soft marketing, with low intrusion can rely on legitimate purposes, whereas more intrusive methods of marketing require consent[112]. The WP has recommended the inclusion of clear situations in which such exception would applies. However, such approach would be over restricted according to business representatives. As stated by ICC: "neither business nor individuals would be well served by an exhaustive list of

[109] Proposal of the Commission

[110] Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95;46/EC/ P April 2014

[111] Recital 47 of the Regulation

[112] Francesco Banterle, IPlens

recognised legitimate interests, which may not anticipate the trajectory of new technology, business model or data use"[113].

As laid down in the Directive and now in the Regulation, legitimate interest of the data controller as a basis for processing calls for a balancing test, between the interest of the data controller and the fundamental rights and freedoms of the data subject. According to the WP, to be considered legitimate, the interests of the controller shall be lawful, clearly articulated and specific enough to allow the balancing test. Once that such requirements are fulfilled, the balancing test must take into account measures as transparency and limited collection of data and key factors as the nature and source of the legitimate interest, impact on data subjects (nature of data), how it is processed, reasonable expectations of the data subject and the status of the data controller and data subject[114].

Thus, it seems clear that the recital does not give a free card for the processing of personal data for direct marketing. The recital states that "the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place." Therefore, the applicability of such provision requires a true balancing test between the interest of the controller and the subjects' rights, which shall take into account the reasonable expectations of the data subjects and their particular relation with the controller[115].

The Regulation does not provide sufficient explanation on what constitutes reasonable expectations. Thus "it may well make sense for companies to refer to such 'reasonable expectations' in their individual data protection declarations or privacy statements and, thereby, to include them into the scope of this criterion[116]".

Nonetheless, the interpretation of recital leads to the assumption that such exception is applied mainly in cases where a relationship between the consumer and the data controllers gives the consumer the expectation that he might receive some advertisement of the company. For example, when the consumer buys a product in a store and it register in the system of such

[113] ICC Position on Legitimate Interests, Policy Statement, ETD/STM – 20 October 2015

[114] Opinion 06/2014

[115] https://iplens.org/2016/07/12/personal-data-processing-for-marketing-purpose-under-the-new-gdpr-consent-v-legitimate-interest-and-recital-47-first-thoughts/

[116] https://www.exchangewire.com/blog/2016/05/24/gdpr-whats-relevant-for-the-use-of-cookies-identifiers-in-online-marketing/ -

store, he is expected to get information about new products or discounts. Thus, it does not seem that such exemption would be applicable to behavioural advertisement.

3.4.5. Profiling

The treatment of profiling in the new regulation was highly debated during the legislative process. Not surprisingly, both, privacy advocates and representatives of the industry, have heavily participated in the negotiations involving the draft of profiling's provisions, given the relevance for the industry to maintain some flexibility on the collection of data for profiling on the one hand, and the importance of providing stronger privacy regulation on the other hand.

The text, as introduced in the proposal of commission, provided "natural person" the right to not be subject to a "measure" which produces legal effects or substantially affects the "natural person", and which is based solely on automated processing intended to evaluate certain personal aspects relating to this "natural person" or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

The provisions set out in the proposal were subject to critics by both, privacy advocates and the industry, mainly regarding to the lack of sufficient definition of key provisions such as "producing legal effect" or "significantly affects". According to the IAB UK, the language proposed by the Commission "potentially (and unhelpfully) includes some forms of online behavioural advertising".24. The IAB UK has raised several concerns about an over restriction on profiling in the new regulation. Similarly the Centre for Democracy and Technology has agreed with the industry that the vague language of Article 20 was "overly expansive and provides little certainty to companies about what sorts of activities are prohibited"..27

On the other hand, Working Party has found that the text did not go far enough and has suggested that the application of article 20 should cover, for instance, web analysing tools, tracking for assessing user behaviour, and creation of personal profiles by social networks[117].

The text of the proposal has gone through changes in the Parliament, including the addition of a profiling's description in article 4 and a prohibition of profiling with the effect of "discriminating against individuals on the basis of race or ethnic origin, political opinions,

[117] Opinion 01/2012 on the data protection reforms proposals

religion or beliefs, trade union membership, sexual orientation or gender identity". However, the final text of the regulation has subsumed mainly the text proposed by the Council in its General Approach, which provided that "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

Interestingly, the final text of the regulation has brought an innovation regarding profiling, namely the provision of article 21, concerning the right to object to direct marketing. Article 21 (2) establishes that when "personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing".

The fragmentation of profiling within direct marketing, i.e., the inclusion of paragraph 2 in the article 21, raises questions on whether profiling for marketing purposes is not deemed to produce legal effects or significantly affects data subjects. At least it gives sufficient arguments to the industry rely on the article 21 (2) when profiling for online behavioural advertisement.

Notwithstanding, the meaning of "produce legal effects" and "significantly affects" deserves a deeper analysis.

Recital 71 of the Regulation mentions two examples as legal effects, namely automatic refusal of an online credit application or e-recruiting practices without any human intervention,

Therefore, it seems sufficiently clear that profiling for the purpose of analysing the data subjects behaviour or financial conditions in the context of changing price of products or services will fall within the scope of profiling as laid down in article 22. Hence, raising insurance prices or refusing credit application produce legal effects or substantially affects the data subject, which triggers the application of article 22 of the Regulation.

Although it seems reasonable to assume that profiling for the purpose of marketing does not produce legal effects or significantly affects data subjects, some extreme cases can be difficult to evaluate.

For instance, one real case involving profiling has gained media attention and it can challenge the assumption that behavioural advertisement does not produce legal effects or significantly affects data subjects: One girl received a coupon targeted to pregnancy woman. Such coupon was sent by a company to women who behaviour and costumes had matched some patterns of

pregnancy. The girl's father has seen the coupon and called the company to complain. Later on, the father has apologized with the company, as the girl has found to be pregnant[118].

In such case, a profile was built with the aim of offering advertisement. It is difficult to say whether such advertisement based on profiling has produced legal effects or has significantly affected her, yet it has undoubtedly caused some discomfort and awkward situation.

Using a hypothetical situation as an example: let's assume that a couple shares the same computer. One day the woman is browsing and is targeted with an advertisement about jewelry sales. After accessing the browsing history, she finds out that the boyfriend has accessed website of a famous jewelry. She might assume that he will propose to her or, in the worse scenario, that he is buying jewelry to another woman. One way or another, it is difficult to assess how this situation can affect data subjects.

Such scenario, although hypothetical, is totally feasible in Big Data era, when decisions are made by algorithms and there is no limit for the amount of data available in the online environment.

The assessment of whether profiling for marketing purposes produce legal effects or significantly affects data subjects has relevant implications, as the legal to object provided in article 21 (2) relies upon a opt-out regime whereas profiling under article 22 requires explicit consent.

Indeed, the Regulation has brought some flexibility to the industry in the conduction of marketing activities based on profiling. However, the legal loopholes of the Regulation can be dangerous to business.

3.4.6. Summary of Relevant Provisions of the GDPR to Online Behavioural Advertisement

Although the GDPR has brought new obligations to data controllers and more strict rules on the processing of personal data in the digital context, the final version of the regulation is significantly less intrusive than the proposal introduced by the Commission and the version amended by the Parliament.

[118] http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#279db25a34c6

The GDPR means to assure data subjects more transparency and self-determination, which means that the industry will need to provide more information and rely on more transparent tools on the obtainment of consent. Agents will not be able to rely on terms and conditions or browsing settings to prove consent anymore and will not be able to hide the purposes of the processing of data. Consent requirements are now more restrict and users shall be more empowered on taking decisions online.

On the other hand, industry still will have some flexibility to conduct business and to place advertisement based on profiles. The GDPR has brought an important innovation pro industry, namely the possibility of direct marketing being found as legitimate interest of data controller for the processing of data.

Furthermore, the industry has some basis to use a opt-out tool on profiling for marketing purposes, based on article 21 (2) of the Regulation. However, it is important to take into consideration potential effects to data subjects. Therefore, data protection assessment will be more important than never.

3.4.7. The European Regulation in Comparison to the US Regulation

Given the importance of the United States on the foundation of the Internet and as the home country of the main tech industries as Google and Facebook, it is important to analyse how the US deals with privacy and how it balances its citizens' rights with economic interests.

Such analysis shall take into consideration that European Union and United States have significant historical and cultural differences. While European Union usually has a more restrict regulatory approach and stronger protection on citizens' rights, the US approach gives more flexibility to companies and relies in values as free market and economic power.

Unlike European Union, United States does not heavily regulate privacy and data protection. There is no provision guaranteeing the right to privacy and data protection in the American Constitution, insofar as the closest reference to the right of privacy is the 4th Amendment, that assures citizens the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Such provision, however, applies only for the right of being not subjected to interference of governmental institutions and is not applicable in the context of commercial activity.

The legal framework regarding privacy and data protection in US is said to be "somewhat disjointed and piecemeal[119]", as legal provisions are divided in a variety of statues and specific sector regulations, such as financial or health information, or electronic communications. The US approach relies mainly on different state laws and self-regulation guidelines and frameworks[120].

The lack of reference of privacy and data protection as fundamental right or in a federal law has led to some criticism and unfavourable comparison to the US regulation in relation to European Union Law[121]. However, the lack of reference as a fundamental right does not mean that privacy and data protection has not been enforceable in the federal level. Besides the existence of several regulations on different States, the Federal Trade Commission has been playing an important role on the enforcement of privacy and data protection rights in the federal level[122].

Among the laws enforceable by the FTC are the Federal Trade Commission Act, the Fair Credit Reporting Act, the Gramm-Leach-Billey Act and the Children's Online Privacy Protection Act. The most relevant for this paper, however, is the Federal Trade Commission Act.

The Federal Trade Commission Act (15 U.S.C. §§41-58) provides consumers protection on a federal law basis and prohibits unfair or deceptive practices. It has general reach, including to offline and online privacy and data security policies. Under the FTC Act, the FTC can initiate an investigation, issue a cease and desist order, file a complaint in court, obtain an injunction, restitution to consumers, and repayment of investigation and prosecution costs.

Besides the FTC Act, the FTC provides several Reports and Guidelines, that although are not directly enforceable, contains relevant guidelines to self-regulation and better practices to business. Particularly in relation to online behavioural advertisement, the FTC has issued the Report on Self-Regulatory Principles for Online Behavioral Advertising. Although the principles are not legally binding, it requires members of various advertising industry trade

[119] Avner Levin and Mary Jo Nicholson; Privacy in the United States, the EU and Canada: The Allure of the Middle Ground; University of Ottawa Law & Technology Journal, 357 (2005)

[120] Lauren B. Movius and Nathalie Krup; U.S and EU Privacy Policy: Comparison of Regulatory Approaches; International Journal of Communication 3 (2009), 169-187; available at http://ijoc.org

[121] Ibid.

[122] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy

groups to comply with the groups' guidelines for online behavioural advertising, which largely mirror the FTC's guidelines[123].

Main provisions of the Report

Online behavioural advertisement is described in the Report as the tracking of consumer's online activities over time with the aim of delivering targeted advertising[124]. While the Report recognizes the privacy concerns on the massive collection of data in the digital environment, it also recognizes the value of behavioural online advertisement, namely the possibility of companies to provide free content that online advertising supports and personalization of advertising to consumers. Accordingly, the report states the necessity of "addressing practices that raise genuine privacy concerns without interfering with practices – or stifling innovation – where privacy concerns are minimal".

An interesting approach is given by the Staff in relation to the scope in which the Principles should apply, i.e., whether only to personally identifiable data, or whether it should equally applies to non-personally identifiable information. After evaluating arguments of several stakeholders, the Report has concluded that the Principles should apply to data that "could reasonably be associated with a particular consumer or computer or other device, regardless of whether the data is "personally identifiable" in the traditional sense." According to the Report, the rapidly changing technologies have decreased the line between PII and non-PII. Thus, as stemming from the conclusions of the Report, information stored in terminal equipment, as cookies, and IP Addresses falls within the scope of the principles outlined in the Report.

The approach of the Report seems to be aligned with the approach given by the Working party 29, in definition of IP addresses and cookies as personal data and equally on the treatment of data that can be associated to a particular consumer or device.

Another interesting approach of the report relates to first party online behavioural advertisement[125] and contextual advertisement. The Report excludes both from the scope of the Principles, as long as data are not sold or shared. In relation to first party online

[123]http://www.loeb.com/articles-clientalertsreports-20090804-advertisingindustryunveilsnewonlinebehavioraladvertisingguidelinesftcallegessearscomandkmartcomfailedtoadequatelydisclosedatacollectionpractices

[124] FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, 2009, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

[125] Ibid.

behavioural advertisement, the Report states that first party behavioural advertising practices are more likely to be consistent with consumer expectation, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites. Accordingly, the direct relationship between consumer and the website give the consumers an expectation that targeted advertisement is placed or at least the understanding of such practice.

Regarding to contextual advertising – advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result, the staff has found that this sort of advertising provides greater transparency than other forms of behavioral advertising and is more likely to be consistent with consumer expectations. The conclusion evidences that it presents minimal privacy intrusion when weighed against the potential benefits to consumers and, therefore, it is likely to be less invasive than other forms of behavioral advertising. Accordingly, staff believes that the Principles need not cover these practices.

At this point, the Report seems more permissive than the European approach. Although the Working Party opinion on online behavioural advertisement focus mainly in third party cookies, it does not exclude first party advertisement and contextual advertisement to the scope of the Directive, as the Report does.

Therefore, the Report focuses mainly in online behavioural advertisement which involves placement of third party cookies. The Report outlines four principles that must be followed by stakeholders engaged on the placement of online behavioural advertisement, namely: i) transparency and control; ii) reasonable security and limited data retention (legitimate purposes); iii) material changes to privacy policies (consent to use behavioural data when it is materially different from premises made when the data was collected and; iv) express consent before using sensitive data.

According to the report, agents engaged on online behavioural advertisement should provide users with concise, consumer-friendly, and prominent statement that: i) data about consumers are being collected at the site for use in providing advertisement and; ii) consumers can choose whether or not to have their information collected for such purpose. Besides, the agents must assure data security and keep any promises that it makes with respect to how it will handle or protect consumer data, even it decides to change its policies later. Particularly to collection of sensitive data, express consent is needed to placement of behavioural advertising.

The Report seems to recommend an opt-out regime on the obtainment of consent to processing data with the purpose of placing online behavioural advertisement. Therefore, its approach is substantially more permissive that the European requirements.

Although the American landscape is less regulate, and even when regulate, it is less intrusive than the European, the FTC has brought important enforcement cases against companies that have failure to provide users with sufficient information and privacy guarantees.

For instance, the FTC has brought cases based on tracking tools place by companies as Nomi Technologies and InMobi, due to practices that allegedly deceived consumers regarding to tracking of theirs locations[126]. Even Google and Facebook have raised actions from the FTC, Thus, the enforcement power of the FTC was found "very effective in practice"[127].

The comparison between European law and American Law shows that while Europe insists in the adoption of strong regulation, the United States focus in soft law and self-regulation, which not necessarily means less effectiveness.

Nonetheless, the adoption of guidelines from FTC, even though nor binding, brings representatives of the industry with clear and easy reading guidelines regarding online behavioural advertisement, whereas the European Regulation contains complex and sometimes ambiguous provisions.

3.4.8 The GDPR in the Light of Fundamental Rights and Economic Perspectives

Given the complexity of the new Regulation and the different nature of the interests involved, it is evident that some provisions will be deemed as too restrictive by the industry or too permissive by privacy advocates. However, the final result of the Regulation seems to have met the interests of both, privacy advocates and industry representatives.

The rapporteur of the LIBE committee, Jan Albrecht, has said the result was a win- is a real win-win outcome and that now "we have a legal environment which creates legal certainty and less bureaucratic burden for businesses[128]". The CEO of IAB Europe, Towsend Feehan has said that "though the new regulation arguably landed in a way that is tougher for publishers and the digital advertising industry, at least the result reflected the various –

[126] https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked and https://www.ftc.gov/reports/privacy-data-security-update-2015

[127] Lokke Morel, pag. 33

[128] https://www.technative.io/gdpr-win-win-says-german-mep-jan-albrecht/

sometimes competing – needs of all stakeholders, from advertisers and agencies through to technology companies and publishers, to civil society[129]".

Many of the provisions of the new regulation seek to assure that fundamental rights are safeguarded in the digital context. The Regulation seems to give sufficient meaning to the Charter, which establishes that "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". The Regulation ensures that personal data is processed fairly and for specific purposes and it has strengthened the conditions for obtaining of consent.

The Regulation could have been more privacy friendly, for instance, maintaining the text of the proposal that foreseen that consent would not be found as a legal basis on the processing of data in cases of imbalance between data subjects and data controller, or not establishing direct marketing as a legitimate interest of the data controller. Such conditions, however, would bring few implications to users whereas it would impose substantial burden to the data controllers and more uncertainty on the conduction of theirs business.

Given the potential economic benefits of a data-driven economy, it is important that companies have some flexibility on the conduction of their business. The GDPR will make some business more difficult and some companies will have to review the way how they conduct business. However, the final text of Regulation does not impose an unfair burden on companies, to the extent of violating the fundamental right of right to conduct business.

In relation to taking advantage of the opportunities emerged within the data-driven economy, some studies reveal that the GDPR may substantially affect the European economy[130]. Indeed, the Regulation does not mean to improve the economic status of European countries. Although the Regulation has maintained important provision assuring some flexibility for business activities, the approach of the Regulation is far from being permissive as the United States legal framework.

[129] http://digiday.com/publishers/iab-europe-chief-theres-obsession-brussels-tracking/

[130] Deloitte, has estimated that over regulating requirements for consent for online behavioural advertisement could significantly reduce jobs (66.000) and the GDP (€ 4.2 billion) https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-european-data-protection-tmt.pdf

4. CONCLUSION

The digital economy has brought several challenges to user's privacy and data protection, as emergence of new technologies has allowed companies to collect and process massive amount of data, some of which are personal. Data as a commodity has led to a data-driven economy, in which many companies rely on the collection and analysis of data in its business activities.

In this data-driven economy, profiling and OBA play an important role as it supports the offer of free services and it entails the offer of tailored advertisement. However, collecting and processing personal data for studying behaviour of consumers and placing tailored advertisement raise serious concerns on protection of fundamental rights, namely the right to privacy and data protection. Given that the currently legal framework on privacy and data protection was not designed to deal with the new technologies currently in place, the European Union has passed a new Regulation on the treatment of privacy and data protection.

In comparison with the previous legislation, namely the DPD and EPD, the Regulation has brought more safeguards to consumers and more obligations to data controllers. In relation to profiling and OBA, the main changes brought by the Regulation are: i) the introduction of IP address and cookies in the scope of personal data; ii) stricter requirements for obtaining consent and; iii) introduction of a definition of profiling and provisions regarding profiling.

Therefore, companies engaged on placing tailored advertisement will have to comply with rules that: i) require that users are given more transparency and information regarding the purposes of which the data will be processed; ii) require that consent is obtained through an affirmative action, which means that companies will not be able to rely on terms and conditions or browsing settings to obtain consent; iii) give the consumer the opportunity of refusing to the process of personal for marketing purposes, including profiling.

Yet, some provisions of the Regulation bring some flexibility to agents engaged on OBA to maintain its activities and to explore the data-driven economy. Under the Regulation, direct marketing might be placed on the basis of the legitimate interest of the data controller whereas profiling for direct marketing was given different treatment in relation to profiling that produces legal effects or substantially affects data subjects.

Undoubtedly, the GDPR enhances the protection of privacy and data protection in the digital context, as it provide clearer definition on new technologies and empower the consumer to be informed and to give meaningful consent to the processing of their personal data. Therefore, it is clear that legislators have given special attention to the fundamental rights of privacy and data protection on the new Regulation and consequently has raised the meaning of such rights.

On the other hand, the Regulation has not ignored the economic potential of the exploitation of data as a relevant source of revenue, innovation and employment. The Regulation has given attention to the right to conduct business and the importance of given companies some flexibility.

Such flexibility, however, is limited. Although some privacy advocates argue that the Regulation could have gone further on the protection of privacy and data protection, it is likely that more restrictions on the business activities could bring severe impacts on the European economy. In this sense, the US provides less regulation that Europe and consequently more business opportunities.

Therefore, the GDPR seems to provide substantial safeguards on the protection of privacy and data protection. It is likely to be the most developed set of rules regarding privacy in the world. Moreover, the Regulation has taken into consideration the importance of exploring the opportunities of a data-driven economy to foster the European economy. Although the Regulation does not give the same level of flexibility to business as the US, the European approach seems to provide a better balance between relevant and antagonistic rights.

Table of Reference

Treaties/Statutes

- Treaty on the Functioning of the European Union
- Universal Declaration of Human Rights
- International Covenant on Civil and Political Rights
- European Convention of Human Rights
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- Charter of Fundamental Rights of the European Union
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Directive 95/46/EC
- Directive 2002/58/EC
- Directive 2009/136/EC
- Proposal COM(2012) for Regulation of the European Parliament and of the Council
- Regulation (EU) 2016/679 – General Data Protection Regulation
- Federal Trade Commission Act (15 U.S.C. §§41-58)

Case Law

- ECJ C-101/01 Lindqvist, 10/01/2004
- ECJ C-70/10 Scarlet v Sabam, 24/11/2011
- ECJ, C-582/14: Patrick Breyer v Bundesrepublik Deutschland, 19/11/2016
- ECJ C-283/11 Sky Österreich GmbH v Österreichischer Rundfunk, 22/01/2013
- ECJ C-360/10 SABAM v. Netlog, 16/02/2012
- ECJ C 131/12 Google Spain v AEPD and Mario Costeja González, 13/05/2014

Working Party Opinions and Reports

- Cookie Sweep Combined Analysis – Report, Adopted on 3 February 2015 – 14/EN WP 229
- Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting
- Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC
- Working Document 02/2013 providing guidance on obtaining consent for cookies
- Opinion 01/2012 on the data protection reform proposals
- Opinion 2/2010 on online behavioural advertising

Books, Articles and Journals

- **Clarke, Roger**. Profiling: A Hidden Challenge to the Regulation of Data Surveillance, Journal of Law and Information Science, December 1993 https://digitalcollections.anu.edu.au/bitstream/1885/46248/31/07Paper06.pdf
- **Krishnamurthy, Balachander and Willis Craig E.**, On the Leakage of Personally Identifiable Information Via Online Social Networks, 2009, http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf
- **Gutwirth, Serge., Leenes, Ronald., de Hert, Paul., Poullet, Yves**, European Data Protection: In Good Health?, Springer Netherlands, 2012
- **Corea, Francesco,** Big Data Analytics: A Management Perspective, Springer, 2016, page 2.
- **Koops, Bert-Jaap**, 'The Trouble with European Data Protection Law' International Data Privacy Law, doi: 10.1093/idpl/ipu023, 29 August 2014.
- **Hildebrandt, Mireille, Gutwirth, Serge**, Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer Netherlands, 2008
- **Corea, Francesco,** Big Data Analytics: A Management Perspective, Springer, 2016, page 2.
- **Hijmans, Hielke**, "The European Union as Guardian of Internet Privacy, The Story of Art 16 TFEU", Springer, Law, , Vol. 31, 2016, page 4
- **Borghi, Maurizio, Ferretti, Federico, and Karapapa, Stavroula**, 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK', International Journal of Law and Information Technology, 21 No. 2, 109–153, 2013

- **Bygrave A Lee**; Data Protection Pursuant to the Right to Privacy in Human Rights Treaties; International Journal of Law and Information Technology, 1998, volume 6, pp. 247–284

- **Borghi, Maurizio, Ferretti, Federico, and Karapapa, Stavroula**, 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK', International Journal of Law and Information Technology, 2013 Vol. 21 No. 2, 109–153

- **Clifford, Damian**, EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour 5 (2014) JIPITEC 194, para 1

- **Groussot, Xavier and Petursson, Gunnar Thor and Pierce, Justin**, Weak Right, Strong Court - The Freedom to Conduct Business and the EU Charter of Fundamental Rights. Lund University Legal Research Paper Series No 01/2014, April 23, 2014 https://ssrn.com/abstract=2428181, http://dx.doi.org/10.2139/ssrn.2428181

- **de Her Paul de Her and Papakonstantinou, Vagelis**, The proposed data protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals,z Computer Law & Security Review 28 (2012) 130-142)

- **Castro, Daniel and Mcquinn, Alan**, The Economic Costs of the European Union's Cookie Notification Policy, the Information Technology and Innovation Foundation, 2014

- **Kirsch, S. Matthew**, Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising, 18 Rich. J.L. & Tech. 1. 2011-2012

- **Moerel, E. M. L.,**. Big data protection. Tilburg: Tilburg University, 2014

- **Borgesius**, **Frederik J. Zuiderveen,** Personal data processing for behavioural targeting: which legal basis? International Data Privacy law, 2015

- **Carolan, Eoin**, The continuing problems with online consent under the EU's emerging data protection principles, Computer Law & Security Review 21 (2016) 462-473

- **Levin, Avner and Jo Nicholson, Mary;** Privacy in the United States, the EU and Canada: The Allure of the Middle Ground; University of Ottawa Law & Technology Journal, 357, 2005

- **Movius, Lauren B. and Krup, Nathalie;** U.S and EU Privacy Policy: Comparison of Regulatory Approaches; International Journal of Communication 3 169-187; 2009; http://ijoc.org

- **Ciriani, Stéphane**, The Economic Impacts of the European Reform of Data Protection, Communications & Strategies, 2015, Issue 97, p.41(18)

- **Zuboff, Shoshana**, Big other: surveillance capitalism and the prospects of an information civilization; Journal of Information Technology (2015) 30, 75–89. doi:10.1057/jit.2015.5

- **King, Nancy**, Profiling based on mobile, online behavior: a privacy issue, 2010, *http://oregonstate.edu/ua/ncs/archives/2010/dec/profiling-based-mobile-online-behavior-privacy-issue*

- **Gautam, Sohin**, 21st Century Problems: Will the European Union Data Reform Properly Balance its Citizens' Business Interests and Privacy Rights,21 Sw. J. Int'l L. 195 2014-2015

- **Ferraris, Valeria, F. Bosco, G. Cafiero, E. D'Angelo,Y.Suloyeva**, Working Paper Defining Profiling UNICRI) . http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf

- **Ferraris, Valeria F. Bosco, E. D'Angelo** (UNICRI) Internal reviewer: B.J. Koops, The impact of profiling on fundamental rights (Tilburg University) - http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf

- **Vermeulen, Mathias**, Regulating profiling in the European Data Protection Regulation An interim insight into the drafting of Article 20, Centre for Law, Science and Technology Studies (LSTS) Vrije Universiteit Brussel, 01/09/2013

Other sources

- The Great Data Race, How comercial utilisation of personal data challenges privacy. Report, November 2015; Datatilsynet

- Interactive Advertising Bureau. Your Online Choices. A Guide to Online Behavioural Advertisement (www.youronlinechoices.com/uk/about-behavioural-advertising)
- The Economist "Little Brother, Special Report on Advertising and Technology" 13.09.2014,http://ogilvydo.com/wpcontent/uploads/2014/09/20140913_SR_MAILOUT.pdf
- FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising
- The Wall Street Journal http://www.wsj.com/articles/facebook-posts-strong-profit-and-revenue-growth-1469650289
- International Chamber of Commerce - Position on Legitimate Interests, Policy Statement, ETD/STM – 20 October 2015
- European Payment Institutions Federation (EPIF), EPIF's position paper on the General Data Protection Regulation, 2015, page 3
- https://www.exchangewire.com/blog/2016/05/24/gdpr-whats-relevant-for-the-use-of-cookies-identifiers-in-online-marketing/ - **Professor Dr Christoph Bauer and Dr Frank Eickmeier**

- https://iplens.org/2016/07/12/personal-data-processing-for-marketing-purpose-under-the-new-gdpr-consent-v-legitimate-interest-and-recital-47-first-thoughts/
- https://www.privacyinternational.org/node/689
- https://www.helpnetsecurity.com/2016/05/25/gdpr-reactions/
- http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics

- http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#279db25a34c6
- The Wall Street Journal http://www.wsj.com/articles/facebook-posts-strong-profit-and-revenue-growth-1469650289
- Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, ARTICLE 29 DATA PROTECTION WORKING PARTY, Ref. Ares(2014)1206666 - 16/04/2014 (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/annex_one-stop_shop_20130513_advice-paper-on-profiling_en.pdf
- https://www.technative.io/gdpr-win-win-says-german-mep-jan-albrecht/
- http://digiday.com/publishers/iab-europe-chief-theres-obsession-brussels-tracking/
- https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-european-data-protection-tmt.pdf
- https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked and https://www.ftc.gov/reports/privacy-data-security-update-2015
- https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy
- http://www.lexology.com/library/detail.aspx?g=981b312b-3c22-4631-b7d9-a390952efac1