PAPER N. 22
a.a. 2018/2019

Why my Facebook profile is a civil rights issue

Sofia Caruso

Trento BioLaw Selected Student Papers

Jean Monnet European Centre University of Trento
Co-funded by the Erasmus+ Programme of the European Union
Università di Trento Facoltà di Giurisprudenza

I paper sono stati selezionati a conclusione del corso *BioLaw: Teaching European Law and Life Sciences (BioTell)* a.a. 2018-2019, organizzato all'interno del Modulo Jean Monnet "BioLaw: Teaching European Law and Life Sciences (BioTell)", coordinato presso l'Università di Trento dai docenti Carlo Casonato e Simone Penasa.

Why my Facebook profile is a civil rights issue

*Sofia Caruso**

ABSTRACT: Big data and machine learning technology are bringing us to the Fourth Industrial Revolution, but their impact on our daily life is still unknown. This paper aims at addressing questions that users can already experience in their online activities, with the purpose of explaining the marketing approach that motivates them and raising awareness about their collateral damages, with particular attention to individuals' profiling from digital data. Then we will examine the current legal approach to these problematic situations, and whether it could be improved in order to respond better to current and future needs.

KEYWORDS: Digital profiling; one-to-one marketing; GDPR; machine learning; social networks

SUMMARY: 1. A holiday in Paris. – 2. What's in a name? / That which we call a rose / By any other name would smell as sweet – 3. The hidden power of psychological targeting. – 4. A field test: my own Facebook profile. – 5. European Law: current achievements and future developments. – 6. Conclusion

1. A holiday in Paris

A public high school in Italy offers you the opportunity to get in touch with people belonging to a variety of backgrounds; that is the case of my friends and me: we are a group of six girls, and our differences are just evident at first sight. Nevertheless, we are so close that we decided to go on holiday to Paris chez Nicole, who studies there. Briefly, it was quite interesting to notice that Google Search gave us six slightly different search results while looking up for "Paris". Nicole's page left more space to local news, while Leaticia and I got a few ads promoting studying in France, Benedetta more feeds about the Jilet Jaunes, and Roberta and Lisa got touristic websites only. Repeating the experiment with other keywords, we observed analogue results. We have been targeted.

Our research feeds were not striking divergent from each other, but this is just one of the very many cases where we can observe how the contents we are provided online are increasingly tailored to suit us, individually. My friends and I share the same sex, the same age, we are university students, and our characters are compatible to the extent that we have a strong bond: therefore, we are likely to have similar reactions to similar inputs.

What if someone we have nothing in common with conducted the same research? More in general, what is happening on strangers' screens that may be radically different from ours?

In this paper, we will have a brief overview of the mechanisms that regulate phenomena related to the profiling of internet users through their data, with particular attention to Facebook advertising as a typical behavioural targeting platform[1].

* *Student at the University of Trento, Faculty of Law.*

In the second place, we will observe the impact of these new technological applications on offline-life, especially on the exercise of constitutional rights.

Finally, we will address the approach of current regulation, its strengths as well as its weaknesses when confronted with contemporary and future threats to privacy, democracy and liberal freedoms.

2. What's in a name? / That which we call a rose / By any other name would smell as sweet[2]

The reason why Google seemed to know our group of friends was that our online activity left a set of "digital crumbs" over the years, which once pulled together may provide the search engine with a puzzle that approximately looks like us. As a consequence, we obtained search results compatible with what Google thought we would have been more interested.

What happened is just a small reflection of the new business model developed along the years, based on three steps: profiling, personalisation, targeting.

The basic idea of such a model is well conveyed in the expression «one-to-one marketing»[3], whose aim was to increase customer satisfaction and loyalty through personalised products.

In order to implement this approach, suppliers had first to identify their customers, then differentiate them according to their specific needs and expectations, interact with each of them, finally customise their products.[4] These steps remained almost unchanged from the '90, nevertheless something remarkable happened in the meanwhile: the digital data revolution.

Companies compete for attention, and the best way to obtain it is knowing how people's mind works; therefore, an extensive collection of data is pivotal to feed the business. The more gripping the content, the longer the exposition to ads.

Daily life is plenty of tricks that persuade us to indulge in the use of apps and websites (e.g. since December 2013 Facebook News Feed auto-plays its videos to increase interactions[5]).

However, such techniques gain their full reach when tailoring the content on the specific customer, thus, companies need individuals' data in order to identify them better.

Yet it is important to keep in mind that data trackers do not need much information to identify a subject with precision.

---

[1] S. C. MATZ, M. KOSINSKI, G. NAVE, AND D. J. STILLWELL, *Psychological targeting as an effective approach to digital mass persuasion*, in *PNAS*, 114, 48, 2017, 12714-12719.

[2] W. SHAKESPEARE, *Romeo and Juliet*, II, ii, 1-2.

[3] D. PEPPERS, M. ROGERS, *The One to One Future: Building Relationships One Customer at a Time*, New York, 1993.

[4] D. FOWLER, D. PITTA, R. C. LEVENTHAL, *Technological advancements and social challenges for one-to-one marketing*, in *Journal of Consumer Marketing*, 30, 2013, 509-516.

[5] in one year video plays were up 785% and engagement with video posts was up 25% according to the *Social Intelligence Report* ADOBE DIGITAL INDEX | Q1 2014

When speaking of anonymised datasets, we first refer to those not containing name, home address, phone number or other obvious identifiers. «Yet, if individual's patterns are unique enough, outside information can be used to link the data back to an individual. For instance, in one study, a medical database was successfully combined with a voters list to extract the health record of the governor of Massachusetts[6]. In another, mobile phone data have been re-identified using users' top locations[7]. Finally, part of the Netflix challenge dataset was re-identified using outside information from The Internet Movie Database[8]»[9]. Another research analysed 15 months of anonymised locations about 1.5 million people and demonstrated that four spatio-temporal points are enough to identify 95% of the individuals uniquely[10].

Modern information technologies such as the Internet and mobile phones magnify the uniqueness of individuals, further enhancing the traditional challenges to privacy[11].

In the Internet-of-Things World, our own devices become data collectors. Smartphones are probably the most precious source of information about their owners, who are willing to give their consent to enable downloaded apps to perform better. But the many applications of their data usually go far beyond their sight. Average U.S. users have 35 apps installed on their smartphone, and 52% of them are used at least weekly.[12] In Italy, the most downloaded apps connect to social networks (WhatsApp, Facebook, Instagram), though entertainment (Netflix) and dating apps are the ones people are more willing to pay for[13].

Having a quick look into some of these popular apps privacy policies[14], we would notice that – even though they do not share "sensitive data" with third parties – they consent to share with advertising partners the information we published, our location, device and connection information, as well as any other such as demographics and behavioural data as long as provided in the form of "aggregate data" or "pseudonymised data".

Are those pieces of information truly irrelevant? Actually no, they are not.

For instance, from the device model it is possible to infer the owner's income, whether he or she is likely to change it often, its kind of connection. As we already mentioned, geolocalisation and mobility data are

[6] L. Sweeney, *k-anonymity: a model for protecting privacy*, in *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10, 5, 2002, 557-570.

[7] H. Zang, J. Bolot, *Anonymization of location data does not work: A large-scale measurement study*, in *Proc. Int. Conf. on Mobile computing and networking*, 17, 2011, 145-156.

[8] A. Narayanan, V. Shmatikov, *Robust de-anonymization of large sparse datasets*, in *IEEE Trans. Secur. Priv.*, 8, 2008, 111-125.

[9] Y. de Montjoye, C. A. Hidalgo, M. Verleysen, V. D. Blondel, *Unique in the Crowd: The privacy bounds of human mobility*, in *Nature Scientific Reports*, 3, 2013, 1376.

[10] *Ibid.*

[11] *Ibid*.

[12] Think with Google, *How people discover, use, and stay engaged with apps.* https://www.thinkwithgoogle.com/advertising-channels/apps/app-marketing-trends-mobile-landscape/ (accessed 31/03/2019)

[13] *App Annie Retrospective Report* 2017 https://www.appannie.com/en/insights/market-data/app-annie-2017-retrospective/ (App Annie is the leading global provider of data about the mobile market).

[14] Tinder and Lovoo privacy policies have been taken as samples.

among the most sensitive data currently being collected, since they allow to reconstruct individuals' movements across space and time and they can disclose sensitive professional and personal information[15].

3. The hidden power of psychological targeting

Still, the force of personal though anonymised data can go even further.

Until now, we only mentioned recorded data, but thanks to the huge amount of information and the powerful analysis tools that AI and machine learning provide us, the world's attention is turning towards statistically predictable information that can be inferred from such records.

In 2013, researchers at the University of Cambridge's Psychometrics Centre analysed the results of volunteers who took a personality test on Facebook[16] to evaluate their "OCEAN" psychological profile (openness, conscientiousness, extraversion, agreeableness, and neuroticism) and correlated it with their Facebook activity (likes and shares)[17]. They showed that easily accessible digital records of behaviour, such as Facebook Likes, could be used to automatically and accurately predict highly sensitive personal attributes, including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. This information, though not openly disclosed, might be presumed from other aspects of people's lives.

Connections between Likes and personality traits were not always that obvious. While following a page named "I love being gay" may be quite a hint about a person's sexual orientation, the link between "Curly fries" and intelligence is less straightforward indeed[18].

Therefore, while single likes, purchases, or web searches seem inoffensive, they may belong to patterns of behaviour that – when taken in the context of thousands or millions of people – reveal some insights[19].

As fascinating such predictive powers may be, their applications may have more or less noble ends. For instance, it would be possible to detect individuals with higher exposition to depression and cure them in advance, or simply to improve online experience for users; on the other hand, it may expose vulnerable individuals by using information they never consented to share.

The success of this first study caught the attention of the Global Science Research, in cooperation with Cambridge Analytica, which was at the centre a great political scandal in early 2018. Cambdrige Analytica

[15] Y. DE MONTJOYE, C. A. HIDALGO, M. VERLEYSEN, V. D. BLONDEL, *above*.

[16] www.mypersonality.org

[17] M. KOSINSKI, D. STILLWELL, T. GRAEPEL, *Private traits and attributes are predictable from digital records of human behavior*, in *PNAS*, 110, 15, 2013.

[18] I intend to spend a couple of lines specifying that eating curly fries will not turn anybody in a genius: this time the content of the page was irrelevant. The algorithm considered the way contents spread on Facebook (briefly, viewing friends' activity in our News Feed) and combined it with what sociologists call "homophily": since we tend to be friends with people like us, if those who first shared the "Curly Fries" page were smart, its followers were expected to be smarter than the average. See also J. GOLBECK, *Your social media "likes" expose more than you think*, TEDxMidAtlantic 2013.

[19] M. KOSINSKI, D. STILLWELL, T. GRAEPEL, *above*.

wanted to establish a methodology for psychographic profiling of individuals based on social media. Consequently, they were able to micro-target individual consumers or voters with messages most likely to influence their behaviour[20].

Starting from the results of the first study by Cambridge University, another research team lead by Micheal Kosinski tested the application of psychological assessment from digital footprints in psychologically tailored advertisement[21]. The study confirmed that persuasive communication effectiveness increases when designed to match personal features and motivations, as customers were more likely to purchase a product after having been exposed to the ad suiting their character then a random one.

Categories such as sex, age groups, nationality, do not achieve the same results since their market segmentation is coarser and does not take into account more specific features. Conversely, the new approach consents a real implementation of one-to-one marketing.

Once again, this power raises essential ethical questions.

During a presentation at the 2016 Concordia Annual Summit, CA CEO Alexander Nix discussed the power of big data in global elections, and his company's revolutionary approach to audience targeting, data modelling, and psychographic profiling[22]. His assertions are worth being considered while discussing the political consequences of microtargeting.

According to Nix, blanket advertising and mass communication are nowadays nonsense: the core of marketing is personalisation, which sensibly reduces the cost of advertisement while increasing the return investment.

«If you know the personality of the people you are targeting, you can nuance your messaging to resonate more effectively with those key audience groups. […] Communication is becoming ever increasingly targeted. So you will no longer see adverts on products and services that you don't care about; rather you will only receive adverts that not only are on the products and services or – in the case of elections –issues that you care about most, but that have been *nuanced in order to reflect the way you see the world* (emphasis added)[23]».

Although anybody has experienced profiling as the sensation of being followed online by a product we once looked up for, what we are facing now is a new phenomenon that raises questions that cannot be ignored like an annoying ad.

It is a psychological mass persuasion conducted on an individual scale, because manipulation of our perspective on the world is happening taking us one by one, through our *private screens*. While old-fashion

[20] I. JIM, M. J. HANNA, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,* in *Computer*, 51, 8, 2018, 56-59.
[21] S. C. MATZ, M. KOSINSKI, G. NAVE, AND D. J. STILLWELL, *above*.
[22] CA assisted Senator Ted Cruz in his campaign for presidential elections: in 18 months, he revolutionised his performance moving from 5% of consents, with little popularity and even inferior name recognition, to be the alternative to Donald Trump with 35%. Cruz allocated all of his resources adopting three technologies: behavioural science, data analytics, addressable ad technology.
[23] A. NIX at The Concordia Annual Summit NYC 2016.

communication showed the same contents to the mass, nowadays programmes are on-demand, and online contents are delivered on our mobile devices.

Inevitably, this impacts on the exercise of civil and constitutional rights.

Specialised agencies are able to detect subjects more susceptible to specific messages and influence their further action. Such techniques could be adopted to enhance political engagement, as well as demobilise voters from the elections[24].

Furthermore, such manipulation would probably be silent and unperceived, given that the recipients of a message would also be the only ones seeing it.

4. A field test: my own Facebook profile

What was previously said may seem a contemporary version of Orwell's *1984* – just creepier.

Thus, I decided to check it by myself, studying my own Facebook profile with new attention. According to Article 20 GDPR (Data portability), Facebook allows its users to have access to all of the information they have about them. The procedure was intuitive and the title promising: "Your ad preferences, Learn what influences the ads you see and take control of your ads experience".

In order to let advertisers reach some categories of potential clients, FB distinguishes them according to a few general features (Relationship status, Employment, Education), and other aspects they inferred: for example they noticed that I am both a WiFi and a mobile connection user, and that I recently changed my phone. They observed that I travelled quite a lot and I have international friends. They classified my "friend peer group" as "University", tracked my search history, my location history, and I could not alter this information they stored. But I could see and modify my ""ds interests' (obviously) where they collected all the pages that I follow, my likes and shares, and grouped them into categories such as "Food", "News", "Shopping and fashion". Some were just totally wrong, and I pat myself on the back for having misguided FB algorithms.

The goal of News Feed is to deliver the right content to the right people at the right time so they don't miss the stories that are important to them. Ideally, we want News Feed to show all the posts people want to see in the order they want to read them[25].

To sum up, the News Feed is meant to optimise engagement with likeable topics by organising the contents according to our previous interactions. Thus, I may be more exposed to my liberal friends' activities than conservative ones, just because I used to "like" their contents more.

[24] https://edition.cnn.com/2018/05/16/politics/cambridge-analytica-congress-wylie/index.html (accessed 02/04/2019); https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401#/ref-link-1 (accessed 02/04/2019).

[25] https://www.facebook.com/business/news/News-Feed-FYI-A-Window-Into-News-Feed.

Other social media and search engines adopt the same principle, with the result that users ultimately receive reinforcing messages from multiple sources about contents with which they agree. This phenomenon is the so-called *Filter Bubble*[26], namely the personal environment of information where we live in when acting online.

However, even though the Internet gives us what it thinks we want, this may not be what we truly need. Chocolate and deep fried food are very likeable topics indeed, but do they deserve to be at the top of my News Feed? Looking for enjoyable contents, we risk exiling disturbing though more challenging subjects. Indeed, virality has nothing to do with content, but with what people think while enjoying it.[27] Should we build more "ethical" algorithms, which mix uncomfortable and diverse contents with tasty junk news for a more balanced information diet?[28]

The Internet is supposed to provide us with an infinite amount of information: when holding a smartphone, we have the knowledge of the world in our palm. Therefore, we expect to be able to build solid argumentations about a wide range of topics just looking up for them. However, information is never neutral, not even online, with one significative difference with traditional media: that such preference is not always explicit. The problem concerns the mere access to information, which may be put in jeopardy when micro-targeting algorithms hide contents from research outcomes.

The consequences on cognitive freedom are stronger when these mechanisms affect platforms that users choose to build their opinions on controversial subjects, such as Google or Youtube: when typing hot topics, we trust that we will see the most relevant results on top, but search results may be biased without us exactly knowing how. Therefore, we should operate a distinction between "primary" and "secondary" sources of information, depending on whether such websites are used to look up for answers or to gather inputs from previously selected sources, and attach different security standards to the two categories[29].

However, observing online trends one thing is for certain: extreme contents grow very popular in little time. Since they provoke outraged reactions, they get higher shares and great attention, maybe despite being less relevant, less accurate or even false. As mentioned above, virality has a lot to do with feelings, and strong messages have the capability to gather together individuals and gratify them with the sense of belonging to a group.

In the end, we risk assuming a dystopic vision of the world[30], that sometimes is hardly comparable to the real one.

---

[26] E. PARISER, *The Filter Bubble: What the Internet Is Hiding from You*, New York, 2011.
[27] D. NGUYEN, *What makes something go viral?*, TED Salon Brightline Initiative 2017.
[28] E. PARISER, *Beware online "filter bubbles"*, TED 2011.
[29] While Google and YouTube are primary websites, Instagram is a sample of secondary source, since its users are aware that they will only scroll pictures from people they follow.
[30] Z. TUFEKCI, *We're building a dystopia just to make people click on ads*, TED Global NYC 2017.

Additionally, communication escalates when people who formed their opinion within incompatible sets of information meet. Since we expect the Internet to be a complete source of knowledge, we do not doubt our ideas anymore, and our beliefs turn in solid truths well-founded in incontrovertible argumentations: the meeting shifts in a sort of clash of (filter) bubbles.

5. European Law: current achievements and future developments

The digital world increasingly relies on *machine learning* systems, namely the branch of AI aiming at creating programs that have «the ability to learn without being explicitly programmed»[31]. In order for *data mining* processes to analyse, categorise and detect correlations or patterns among data, it is necessary to analyse large amounts of previously collected data[32].

From a merely technical perspective, such advanced computational systems benefit of the full availability of databases from the cloud; on the other hand, this same feature may be problematic to reconcile with the principle of "minimisation" from data protection law.

Data protection raised at the top of the European agenda as a fundamental right to informational self-determination, covered under article 8 of the ECHR.[33] Accordingly, the General Data Protection Regulation is meant to enable individual with better control over their digital activities through lawful, transparent and fair data processing. The GDPR requires such operations to be minimal, related to essential data only and it recommends limited storage time (Article 5).

The material scope of the Regulation concerns "personal data", namely «any information concerning an identified or identifiable natural person», including pseudonymised data «which could be attributed to a natural person by the use of additional information».

Therefore, the definition is broad, and it has the potential to cover very many fields of application; on the other hand, its blurred borders may cause uncertainty in law enforcement.

Indeed, Recital 26 says that «to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used [...] either by the controller or by another person» with regard to «the available technology at the time of the processing and technological developments».

Thus, the compliance test should consist of two parts: the former evaluating purpose, means of processing, interests at stake, risks of technical failures; while the latter would be a "dynamic test" considering «state

[31] A. SAMUEL, A. MUNOZ, *Machine Learning and Optimization*. https://www.cims.nyu.edu/~munoz/files/ml_optimization.pdf (accessed 11/05/2019)

[32] European Data Protection Supervisor https://edps.europa.eu/node/3099#data_mining (accessed 11/05/2019)

[33] ECJ, Judgment of the Court (Grand Chamber) of 16 December 2008, Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, in *ECR 2008, I-09831* (Satamedia). «Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged».

of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed»[34].

Hence, even if identification is not possible here and now (maybe because it requires a disproportionated effort), controllers should anticipate whether non-personal information could turn into a personal one during storage time. Such an operation requires capabilities which do not belong to consumers, neither it is trivial from a data holder perspective.

In the Nowak case[35], the ECJ addresses the notion of information "related to" a natural person. The court adopts an extensive interpretation of the concept, assuming that the use of the terms "any information" «is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments» relating to the data subject. How is this correlation established?

As already mentioned, machine learning provides highly predictive results from apparently useless or generic information. Softwares are growing more sophisticated and efficient one the one hand, while less transparent on the other. It is what Peter Norvig, AI manager at Google, has called «*the unreasonable effectiveness of data*»[36].

Nonetheless, the logic of a self-learning algorithm has nothing in common with human one, nor does its error patterns; therefore it is hard to establish in advance whether there is any relationship between the data and the data subject.

Alternatively, we should rethink all of the data produced by individuals as – potentially – personal data, depending on the contest; or accept that any data may be meaningful, «even if not for humans»[37].

Pursuant to the GDPR[38], data subjects have the right to know and obtain communication from the controller with regard to «the existence of automated decision-making, including profiling […], and meaningful information about the logic involved […]».

Nevertheless, we should consider that machine learning algorithms do not always explain the relation among the pieces of information it clusters together, nor whether there is a causal link between them[39]; it mostly depends on their computational learning model: some allow human to track the way they work (e.g. decision tree algorithms), while others operate as incomprehensible "black boxes" (e.g. neural network

[34] Article 29 Working Party opinion 4/2007 on the concept of personal data, (WP 136).
[35] ECJ, 20 December 2017, Case C-434/16, *Peter Nowak v Data Protection Commissioner*, in Digital Reports (Nowak), §34.
[36] A. Halevy, P. Norvig, F. Pereira, *The unreasonable effectiveness of data*, in *IEEE Intelligent Systems*, 24, 2009, 8-12.
[37] N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 10, 1, 2018, 40-81.
[38] Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR.
[39] M. Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, in M. Hildebrandt, S. Gutwirth, *Profiling the European Citizen*, Dordrecht, 2008, 17-45.

algorithms).[40] Moreover, self-learning algorithms are designed to update themselves while elaborating new data and solutions, so that the original code is meant to change along the way[41].

Therefore, we should clarify the meaning of both "logic" and "meaningful information", as an explanation – comprehensible to the data subject according to his/her technical competences – of the inputs provided to the algorithms and of the criteria working as guidelines for the learning process[42].

To sum up, the European legislator aimed to assign a broad scope to the concept of "personal data"[43], determined by analysing the content of the information, the purpose of the processing and whether such operation may produce effects on the related subject. Excluding a category from such definition would preclude the application of the safeguards observed in the area of personal data protection: quality standards, rights of access, rectification and objection, control by the supervisory authority[44].

As a result, «European data protection law is facing a risk of becoming *the law of everything*»[45], requesting the highest legal protection under all circumstances, but impossible to comply with.

For instance, in previous chapters, we faced phenomena that did not necessarily concern personal data, although it was clear that the effects of processing anonymised information are comparable to those falling within the scope of the GDPR. Technological advancement will sensibly reduce the cases of irreversible anonymity[46], while on the other hand, such sets of data would be subject to analytics mechanisms too.

Therefore, a shift of perspective is yet to come, because the current distinction between personal and non-personal data – which seems to imply that only the former deserves legal protection[47] – will soon become outdated. Indeed, almost any kind of information will have a potential impact on individuals, due to data mining and machine learning analytics.

For example, personal data collected through tracking technologies (e.g. cookies), even in an aggregated or anonymised form, may be compared with the patterns already detected by the algorithms and used to predict other aspects of the data themselves: this way data mining expresses its inferential power[48].

---

[40] D. KAMARINOU, C. MILLARD, J. SINGH, *Machine Learning with Personal Data*, in *Queen Mary School of Law Legal Studies Research Paper*, 247, 2016.
Especially, neural network models are typical of deep learning algorithms. In these cases, their conclusions are «non-deductive and thus cannot be legitimated by a deductive explanation of the impact various factors at the input stage have on the ultimate outcome», see D. R. WARNER in D. KAMARINOU, C. MILLARD, J. SINGH.

[41] *Ibid*.

[42] *Ibid*.

[43] *Nowak*, §34.

[44] *Ibid.*

[45] N. PURTOVA, *above.*

[46] The data is anonymous only when anonymization is irreversible, according to Article 29 Working Party opinion 05/2014 on anonymisation techniques, (WP 216), 3, 5–7.

[47] N. PURTOVA, *above.*

[48] A. FURNAS, *Everything You Wanted to Know About Data Mining but Were Afraid to Ask*, in *The Atlantic*, 2012. http://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/ (accessed 11/05/2019).

Sources of threats are multiplying, and once fully implemented the GDPR will require them to comply with high standards of security that may be even too burdensome, and hence circumvented[49].

A solution may come from the Regulation itself, whose article 35 introduces a data protection impact assessment which «taking into account the nature, scope, context and purposes of the processing» determines whether it constitutes a high risk to the rights and freedoms of natural persons.

Attaching an appropriate risk level to data processing operations would enable supervisory authorities to differentiate their requirements according to a scalable and proportionate approach to compliance.

Indeed, Data Protection Authorities should be empowered with significant control, considering the impact that the data economy may have on people's lives, both as individuals and as groups. When evaluating the risk assessment of a specific process, we should balance it with the constitutional right to privacy, as a mean to preserve the free exercise of democratic liberties.

One-to-one marketing techniques are more likely to circumvent traditionally designed privacy policies, generally based on consent. Despite the reform introduced with the Regulation, consent clauses are the object of an on-going debate concerning the lack of any real alternative, and the fact that they may be incomprehensible to lay people because of their length and complexity. In a comprehensive perspective, we should consider the amounts of data collection processes that individuals are subjected to every day, and whether or not it is reasonable to expect them to actually read, understand and finally give informed consent to every single operation. Significantly, in May 2016, the Norwegian Consumer Council led an experiment[50] to make evident how unrealistic this would be, streaming themselves while reading out loud the terms and conditions of popular apps in an average phone: it took them 32 hours.

Additionally, once implemented with psychographic profiling aimed at targeting people according to their interests, privacy policies will become mere accept-it-all forms.

Finally, in the precise case of decisions based on automated processes, it would be even more critical to determine the value of "specific and informed consent", since it should oblige the controller to provide data subjects with meaningful information about the logic of the ML mechanisms involved, which present relevant obstacles in practice[51].

The magnitude of the rights at stake would justify the empowerment of DPAs. In the previous chapters, we showed a few of the possible application of data-driven technology in influencing political engagement, pivotal choices and the debate between different perspectives. The potential of manipulation through private screens is such that may affect citizens' freedom of thought itself, as well as the right to make free and informed choices: ultimately, democracy at its core.

[49] *Ibid*.
[50] https://www.forbrukerradet.no/side/the-consumer-council-and-friends-read-app-terms-for-32-hours.
[51] See above, note 40 et seq.

Therefore, according to the public law framework of current legislation, DPAs should be able to preserve data subject – namely, their citizens – pursuant to an updated right to mind privacy.

The GDPR already provide us with some useful tools.

As a first thing, it evaluates continuous compliance, along with the duration of the process: EU public authorities may share the results of their investigations through an online platform for monitoring contract fulfilment[52], enhancing compliance with the threat of reputational sanctions, and providing consumers with better grounds to undertake judicial action[53].

In the second place, the Regulation requires purpose-bound terms of contracts. More specifically, the legislator may intervene against standardised forms, which disincentive users from a conscious reading, and require further explanations aimed to contrast future abuses.

In the case of profiling, since it can be used to serve a wide range of purposes, service providers should avoid catch-all purposes such as "providing a personalised service", while "recommending similar age-appropriate video" or "recommending age-appropriate advertising" are better samples of precise indications.

Improving the quality of contracts is crucial and, since European law in this field is publicly-oriented, public authorities should be invested with a role analogue to consumer associations in Business-to-Consumer relationships. They could assume the position of centres of expertise and assistance for individuals, monitor on-going compliance and advice the legislator thanks to their experience on the field.

Analysing the position of social networks, they fall within the scope of the Regulation as data controllers[54], under a principle of factual influence[55] rather than formal arrangements since «they provide the means for the processing of user data and provide all the "basic" services related to user management»[56]. Their role also implies determining the destination of users' data for advertising and marketing purposes.

Therefore, there is no doubt that they have to comply with the legal obligation on privacy, but not all of them are ready to meet all its standards. Mark Zuckerberg already stated his intentions to build «a privacy-focused messaging and social networking platform»[57] and praised the stricter regime of the European Regulation, but Facebook has deep pockets, and it should face fewer obstacles than smaller businesses and

[52] S. VAN GULIJK, J. HULSTIJN, *Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach*, in *European Review of Private Law*, 5, 2018, 635–660.

[53] Another challenging question related to machine learning concerns compliance with the exercise of individuals' rights to rectification and erasure of personal data: what if these data have become part of the learning process elaborated by the algorithm? Should the data controller re-train the algorithm without these pieces of information? And what kind of obligation lies on third-parties that may be responsible for providing the algorithms?
See D. KAMARINOU, C. MILLARD, J. SINGH, *above*.

[54] Article 4(7) GDPR: «controller is the natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data».

[55] Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor", (WP 169), 11.

[56] Article 29 Working Party opinion 5/2009 on online social networking, (WP 163), 5.

[57] M. Zuckerberg in a Facebook post on the 6th of March 2019.

start-ups which cannot count on the same budgets and know-how to address the high complexity of the GDPR.

Sophisticated measures may be in the interests of both the public and influential businesses, but they may draw the long-term risk of a data monopoly that will define irremediable imbalance in future contracts.

Once again, a risk-oriented approach may meet the needs of a data controller whose processing is relatively low-risk with the demand on fewer legal obligations. It is possible to vary accountability tools such as data protection by design and by default (article 25), data breach notification (article 33), security measures, certifications (article 42).

Nonetheless, the rights granted to the data subject - like the right of access, rectification, erasure, objection, transparency, right to be forgotten[58] - should be respected regardless of the results of the risk assessments.

Furthermore, data subjects should be given more options to execute and enforce their rights. In order to fully implement their right to an effective judicial or administrative remedy (articles 77, 78, 79), the European Union should promote the development of collective redress mechanisms. Indeed, despite the broad content of article 80, recognising a right to mandate a not-for-profit organisation or association for both injunctive and compensatory redress, the Recommendation on Collective Redress[59] has already been realised with different outcomes in the Member States: the principle of procedural autonomy may constitute an impediment to exercise of this remedy in practice.

In contrast with this trend, when dealing with machine learning we should probably focus less on the transparency of the procedure, considering that – due to the many problematics inherent in the nature of such computational systems themselves – sometimes "black box" models grant better (more performant) results. However, even though it is impossible to intervene on "hidden layers", we may exert control over inputs and outcomes.

For instance, «by testing the trained model for unfair discrimination against a number of "discrimination testing" datasets, or by assessing the actual outcomes of the machine learning process to prove that they comply with the lawfulness and fairness requirements»[60].

Last but not least, the most effective defence system to privacy intrusions and manipulation of data is knowledge. Since *digital hermitage* would not be a feasible solution to everybody, we should at least raise awareness about the importance of the information that we share.

[58] The right to data portability is still unfeasible from a technical point of view.

[59] Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law (2013/396/EU)

[60] D. KAMARINOU, C. MILLARD, J. SINGH, *above*, 22.

Nowadays we are facing a *privacy paradox*[61]: even though privacy has received a great deal of attention in the media in recent times, users of social networks and apps are keen on sharing detailed personal information on their profiles.

As a first step, people should acknowledge the many potential uses of their data and their economic value; given that, it would be easier to understand how and why persuasive infrastructures can be designed starting from their digital footprints.

The legal framework can support the growth of genuinely consentive users, by means of higher standards of protection and incentives for user-friendly policy designs. Nonetheless, it would be up to the individual to advocate for their right to cognitive liberty[62] and take the measures to preserve their full capability of building their own opinions. Going offline may be an option, at least as a sort of vacation to places where to meet and exchange ideas. Also, mere consciousness may be an excellent antidote to escape Internet echo-chambers where disinformation reigns, and to use the web as a great medium to get in touch with reality instead.

Socials and apps may agree in implementing good practices themselves. They adopt nudging techniques to influence users' choice about privacy settings: what if this system was reversed?

The graphics and the language used to show two alternatives are generally framed to make one more appealing than the other; another way to shape actions consists of making an option cumbersome or time-consuming, encouraging users to prefer the easier one.

A big step forward could be to promote neutral policy design, or even turn nudging techniques into mechanisms aimed at promoting safer and healthier behaviours.

The UK Information Commissioner drafted his proposal of a *Code for Age appropriate design*[63] considering the beforementioned principles. The document provides guidelines on the design standards that providers of online ISS, which process personal data and are likely to be accessed by children, have to meet. Social networks, online games, streaming platforms should set their privacy standards at the highest level by default for users under 18, and should not nudge them into giving away more information than necessary.

One of their suggestions is about profiling and engagement with online contents: they considered that reward loops or positive reinforcement techniques (such as likes and streaks), continuous scrolling, notifications and auto-play features encourage users to stay actively engaged with a service, allowing the online service to collect more personal data; therefore, such options may be disabled for minors. A

[61] S. B. BARNES, *A privacy paradox: Social networking in the United States*, in *First Monday*, 11, 9, 2006.

[62] N. FARAHANY, *When technology can read minds, how will we protect our privacy?*, TED Salon Zebra Technologies 2018.

[63] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services/ (accessed 20/04/2019)

proposal may be to prevent them from "liking" contents, or to use their data exclusively to filter the kind of messages they are exposed to more rigorously.

However, this draft is an excellent example of how law can turn into a tool to raise awareness and protect weaker subjects.

6. Conclusion

The technology that made such data usage possible has been developed according to a specific model of business, whose success and effectiveness makes a change in the digital environment even harder, due to the fact that its functioning lies on learning algorithms that need more and more data to enhance in precision. Yet, it raises issues we can no longer postpone.

The number of IoT devices is expected to grow to 50 billion in 2020, while half of the world population should become a smartphone user by 2021. These disruptive forces have a tangible effect on citizens' rights, such as freedom of expression, freedom of thought, voting, and non-discrimination.

Thus, it is imperative for the European Union to lead the debate about the proliferation of technology in our lives and how it will affect our privacy and our personal and social security.

Even in a context of machine learning and black box processes, it is up to humans to preserve the reliability of these algorithms, with adequate surveillance on the quantity and quality of data used to train them, reference to trustworthy sources and strenuous fight against existing bias. We should keep in mind that the criteria with which algorithms "educate themselves" reflect our values and ethics.

Therefore, we should be aware that the incontestable raise of artificial intelligence will not bring objectivity in our decisions by itself; instead, we can observe that the complexity of human affairs is invading the algorithms[64].

We cannot abdicate and outsource our responsibility to machines, – quite the opposite – we should understand that artificial intelligence is challenging us to question what makes us human.

[64] Z. TUFEKCI, *Machine intelligence makes human morals more important*, TED Summit 2016.