Rome, October 19th, 2020

CIVILTÀ DIGITALE's Contribution for the Public Consultation on the EDPB's *Guidelines 8/2020 on the targeting of social media users, Version 1.0, Adopted on 2 September 2020*

- Non confidential document -

Civiltà Digitale - APS

Sede legale in Roma, Via Matteo Bartoli n°30 - 00143- Roma

WWW.CIVILTADIGITALE.IT Info: **Info@civiltadigitale.it**

Association description

Civiltà Digitale is a non-profit association for civic, solidarity and social promotion purposes, legally established pursuant to the art. 35 of the Italian legislative decree n. 117 of 2017 (Italian 3rd sector code).

It operates as an independent and apolitical think tank aiming to provide concrete intellectual support for the digital development of the Italian and European society, through the aggregation of heterogeneous experiences, innovative ideas and cultural contribution of its members and associates. A holistic approach and an interdisciplinary contamination are Civiltà Digitale's main strengths: we believe that sharing information, advice and vision with citizens and institutions could lead to digital users' wellbeing.

Among others, Civiltà Digitale carries out activities in the following fields: education, training, scientific research, arts & culture, protection and promotion of human, social, civic, consumer rights and equal opportunity.

Contact Person:

For any question related to this document, please contact Civiltà Digitale's secretariat at info@civiltadigitale.it .

Summary

1. Introduction to Civiltà Digitale's contribution

Profiling activities related to user targeting goals on social media platforms (SMP) can lead to a loss of control over users' personal data, just as lack of transparency on the roles and powers of the various actors involved in these activities can hinder the exercise of the rights by digital users. With such concerns in mind, Civiltà Digitale decided to take part in the public consultation on the EDPB's guidelines on the targeting of social media users to provide its contribution towards the achievement of a shared set of best practices for the involved actors that can affect digital users' wellbeing.

Our *Digital safety* workgroup analysed the EDPB's guidelines and collected some proposals to improve their effectiveness. In particular, we identified the following issues:

- privacy and transparency notices often prove to be not fully or easily understandable by non-expert users, either because of the technical/legal jargon they use or due to an information overload caused by their length or complexity (i.e., too many layers);
- cutting edge techniques of data processing available to SMPs could allow third parties to indirectly identify users even beyond reasonable expectations;
- distribution of responsibility among actors involved in data management processes is often unknown to non-expert *targeters*;
- easy-to-use tools offered to users to exercise their data management-related rights are often provided by external software houses, which can claim their products as "sufficient" to comply with GDPR (whereas they may only be useful) and would become an additional actor in the data management process.

These topics, along with our points of view and suggestions, are detailed in the following paragraphs.

2. On the risks to the rights and freedoms of users posed by the processing of personal data

Targeting of social media users may involve use of personal data that goes against or beyond individuals' reasonable expectations, thereby infringing GDPR principles. It is our belief that users, as data subjects, should be informed on the risks of data processing with understandable privacy notices (1 or 2 layers maximum) before joining any social media platform. In any case, the first and the foremost message conveyed should denote how control over users' data is guaranteed by the data controller to users themselves, then how processing of personal data is performed by the SMP. In practice, this can be fulfilled specifying *where* information is stored and processed (in EU or extra-EU countries), through a clear and evident disclaimer.

For what concerns data processing, the risks to the rights and freedoms of users should be further analysed with respect to the concept of personal data as information which may lead to an identifiable natural person, namely who can be identified indirectly by advanced data processing techniques. To this respect, we believe that EDPB could point out the role of data science, in particular the analysis of big data sources through data mining techniques[1]. As a matter of fact, the extraction of data patterns can lead to unauthorized access to personal data and undesired discovery of information of interested persons: these are unexpected information that could significantly exceed individuals' reasonable expectations, violating the GDPR principles. To this end, the EDPB's document could include references to Privacy-Preserving Data Mining (PPDM) techniques. Similarly, reporting in the Guidelines the role of the most relevant PPDM techniques from the literature can bring to analyse typical applications of PPDM methods in relevant fields[2]. This is particularly important since EDPB acknowledges that the potential for

[1] J. Han, M. Kamber and J. Pei, Data Mining: Concepts and Techniques, San Mateo, CA, USA:Morgan Kaufmann, 2006.
[2] R. Mendes and J. P. Vilela, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications," in *IEEE Access*, vol. 5, pp. 10562-10582, 2017, doi: 10.1109/ACCESS.2017.2706947.

discrimination in targeting arises from the ability for advertisers to leverage the extensive quantity and variety of personal data that social media platforms gather about their users.

Furthermore, we sustain the existence of risks related to so-called 'filter-bubbles', within which users are exposed to 'more-of-the-same' information and encounter fewer opinions. We also agree on the fact that targeting mechanisms may also create risks of "information overload", whereby individuals cannot make an informed decision: too much information equals non-information, a concept that should be reflected in transparency mechanisms used by data controller and processors. Online platforms often have layered notices, but such mechanisms should be carefully used (or in some cases avoided), since too many layers are *de facto* a similar obstacle to end users' information needs.

3. On data protection actors

Civiltà Digitale agrees with the EDPB on the concept that controllers may be involved at different stages of the processing of personal data and to different degrees. However, the level of responsibility among actors is often unknown by "small targeters" due to their low level of knowledge of GDPR and privacy implications of social media features (e.g. Like on Facebook). We suggest to examine the actual situation of micro and individual businesses (SMEs), where budget constraints can limit the possibility of access to privacy training or professionals support. In this respect, the request to controllers to put in place an arrangement which transparently determines their respective responsibilities for GDPR compliance should be, in case of joint controllership, primarily addressed to SMP owners.

The EDPB correctly recalls that the use of generic purposes, like "advertising", would result in broad definitions unable to fully inform users on data processing activities. We sustain the principle that it should be made transparent to data subjects what types of processing activities are carried out and what this actually means for them. We suggest to point out that the use of hypothetical or future purposes is not correct as well: as a matter of fact, the collection of data for possible future purposes is against the principle of minimization, which states that where personal data is needed, it should be limited to what is necessary for the purpose.

Regarding the right of access, we are concerned by the broad interpretation that could be assigned to the sentence "An easy-to-use and efficient tool should be available for the data subject to ensure the easy exercise of all of their rights" (par. 92). The Art. 24 of the GDPR states that the controller must take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. This means

also in terms of right-to-access tools. Most large SMP already correctly offer a dashboard through which users can manage their data, but small targeters may not be able to autonomously provide such tools and would hence outsource these features to external software houses (e.g. by using a plugin they provide). This may result in risks of a twofold nature:

i. software houses can claim their products as sufficient to comply with GDPR (e.g. products advertised as “all-in-one GDPR compliance plugin”), whereas they may only be useful, as supplementary measures may be requested to the targeters;

ii. software houses would become an additional actor in the data management process, further complicating the scenario for data subjects.