Opinion on EDPB's Draft Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

This opinion only reflects the views of its author.

The *Draft Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)* (hereinafter: Draft) raise several questions. Here are the most critical ones:

1. First of all, it was surprising to read that according to the Draft, *"search engine providers' activities are **likely*** [emphasis added] *to fall within the scope of direct provision of ISS"* (information society services). Well, not really: it has been "sure", "obvious", "without doubt", "out of question" for long time that search engine providers' activities are within the scope of direct provision of ISS. This, however, drastically changes the way how this issue should be handled. Obligations under Article 12 of the Directive 2000/31 cannot be considered as compatible with obligations under Article 17 of the GDPR. In other words – see further comments below –: it should be not the search engine providers' obligation to erase the data, but that of the entity originally publishing it (as it is not the dish "who" is responsible for a tasteless meal but the cook instead). And this would be simpler and more logical and more legal (i.e. the entity originally publishing the data can decide if the reason of publication is still valid or not) than overcomplicating this issue…

2. Even if this issue is intended to be handled under the GDPR, it should be realised that the ***name itself is not an identifier***, therefore reducing the question to *"erase one or more links to web pages from the list of results displayed following a search made on the basis of his or her name"* is pointless. To illustrate it: there are 17 people with the name of "Bártfai Zsolt" in Hungary, information of many of us can be found on the internet. If I asked the search engine provider to remove all information on "Bártfai Zsolt" from the list of results displayed following a search, the rights and interests of 16 other "Bártfai Zsolt"-s would be violated, maybe, for example, those of an entrepreneur for whom being on such list may result in economic benefit, and vice versa: I would not be happy if – upon request of another "Bártfai Zsolt" – my articles were not easier accessible. So, an action by a person with a given name may easily create conflict(s) with other data subject(s) whose rights are not less important.

3. It is not logical to deal with search engine providers only, because the key issue is (should be) the ***source of the information*** found by the search engine. If it is true that the data may remain on the original websites and it must be removed only from the list of results displayed following a search, what does this solve? Does it exclude the access to, and dissemination of the same data found on the internet? No. Will the latter be illegal? No. May it violate the freedom of expression and information or the right and interest of others, as well as the interests/reasons, maybe laid down in legal rules, behind the publication of data? Yes.

4. The focus should, therefore, be on the ***process leading to, and the moment of, publication*** of the data. Because the data controller publishing the information should comply with the

data protection legislation and its activity(ies) (may) fall(s) under the GDPR (or any data protection legislation). It is a legitimate question whether the GDPR is about regulating "data processing" in the public (i.e. from the moment of publication). It has been my opinion for long time that the "public" is a "one-way street": a data can become public but after that the same data cannot become "private" again ("the internet does not forget"); neither legally, nor technically (not even if the CJEU or the EDPB make efforts in that direction). In other words: if something has become public that will remain, in fact, public.[1] And, in the public none of the rules of the GDPR can really be applicable, the provisions of the GDPR (or that of any data protection legislation) applies *before* the data has been made public. That is, in the public we cannot speak of "what is allowed only" (cf. GDPR/data protection legislation, especially conditions described in Articles 13&14), but on the contrary: "what is not allowed to be done with the data" (i.e. to violate the moral rights protected by civil law).

Some explanation: making a data public must have a purpose – more precisely a reason –, but this reason is no longer relevant after the publication because the "public" (i.e. each and every single person having access to this information) has/might have completely different motivation when the data in question are used (education?, research?, protection of economic or other interest?, simply entertainment?): how the public should know the original reason for publication? How could it be ensured that any single person uses the data for the same "purpose" as determined by the entity publishing the data? Further, the *real* data controller (i.e. who determine the "purpose" of using the data that has become public) is not the search engine provider, but rather the person who initiates the search (even if CJEU declared the search engine provider as data controller): the search engine provider provides only the "means" but the purpose is determined by the person initiating the search (and this raises whether is it not joint controllership?). Further, if the baseline were "what is allowed only", events in the public would have to be regulated from the beginning to end. This is not technically feasible, nor constitutional.

Entity making a data public may be responsible for violating the data protection legislation, but nobody else. I firmly believe that in the public legal protection is no longer provided by the data protection legislation but by other branch(es) of law, e.g. the civil law or even the criminal law: I, as a person having found a data on the internet by using any search engine, cannot ***use*** this data against the data subject in such a way that violates his/her moral rights (and only the use of such data can be prohibited, not the possession/knowledge of it..).

4. Article 85 of the GDPR also supports this interpretation. This is the provision in the GDPR which ***obliges the Member States*** to adopt legislation to *"reconcile the right to the protection of personal data … with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression"*. Since Member States may derogate from (actually) any substantial provision of the GDPR, this area – i.e. the right to freedom of expression and information, including

[1] That is why Article 17(2) is senseless: something is "public" because the person who makes that data public provides the data to *anybody*, without examining who will have access to those data and/or without keeping a record of such persons who have had access to that. How the obligation in Art. 17(2) is intended to be implemented? Via a new public statement – because the "recipients" are, *per definitionem*, unknown – making public again the personal data that should not be used any longer?

processing for journalistic purposes and the purposes of academic, artistic or literary expression, inc. the data processing in relation to these activities – is (can be considered as), ***in fact, out of the scope of the GDPR***. It is necessary to emphasise that, since Member States may derogate from the provisions of the Article 17 of the GDPR as well, there is no exact legal framework against which this issue could be assessed. This raises also the question if the EDPB has any authority to issue this Guidelines, since the core issue in this regard is not the interpretation of the GDPR [cf. Art. 70 (1e)] but that of the Member States' legislation (or the Draft may choose the option to emphasise that everything therein is "without prejudice to Member States' legislation on the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression").

* * *

In sum, this issue is more complex than as wrong CJEU judgements and EDPB guidelines treat it. And this Draft is, again, an evidence for the approach of data protection legislation being considered as "super law". Hopefully, it will come soon when it is realised that

a) data protection legislation is not suitable for all cases, and
b) even GDPR (or any data protection legislation) is not suitable for all cases where personal data are "processed".

by Zsolt Bártfai (one out of the seventeen)