Guidelines 3/2022 on

Dark patterns in social media platform interfaces: How to recognise and avoid them

Version 1.0

Adopted on 14 March 2022

for public consultation

The Guidelines in question are significantly useful in terms of describing and helping to recognize the main dark patterns in social media platforms.

There is, indeed, a large number of examples indicating the real case scenarios occurring in practice in social media platforms interfacing.

The object of the Guidelines represents an intelligible matter for the public (as it is related to the interaction with social media platforms) and the main aim is to provide recommendations and guidance for the design of the interfaces of social media platforms.

In connection with the main aim of the Guidelines, the social media providers (as data controllers) are the main addressees of the soft-law in question as they have to fulfill the GDPR principles since the beginning stage of a life cycle of a social platform designing.

Remarkably pointed out (one of the main spirit of the reasoning in coherence with the GDPR philosophy) at par. 127 of the Guidelines: "*social media providers might argue that the least invasive setting would defeat the goal that users of a particular social media platform have, for example being found by unknown people to find a new buddy, date or job. While this might be true for some particular settings, social media providers need to keep in mind that the fact that a user uploads certain data on the network does not constitute consent to share this data with others*".

It is clear from the content of the Guidelines that, currently, in the majority of social platforms, the users are facing all the issues indicated and described. In addition, to all the clear examples listed (that obviously cannot be exhaustive) there would be other issues to be highlighted.

For example, in the registration process of a social media, it would be important to stress also the fact the providers should make the best effort in order to ensure the real identity of the user that is asking the registration in the platform. The real identity of the person, indeed, represents a core issue in order to protect the persons and to prevent the creation of fake social networks user identities (plus, obviously, the specific topic of the identity of the children with all other connected aspects of the matter).

Strictly related to the above point, it would be also important to add specific guide on the eventual facial recognition pattern as this is becoming very popular in the platforms for several aims indicated by the providers, like: strong authentication, authorization of actions, opening / accessing the platform (mostly via the mobile app version used from the smartphone).

Other important points could be the fact that the majority of social media providers are "big giants" in the market with the consequent issue regarding the location of the servers and all the aspect regarding the transfer of data. Although other Guidelines face the issue of transfer, it would be useful to recall and also to point out some specific guide in the context of the Guidelines in question also.

In terms of concrete common scenario, it would be useful to indicate also another common case occurring in social platforms that is about the eventual disturbing (or "stalking") via text messages. It would be necessary that providers make the real best effort in order to set the platform since the beginning with the less intrusive pattern way in messaging. For instance, the providers should set the messaging pattern since the registration phase, allowing the user the choice to receive messages only from other users "friends" and not by anyone. Same reasoning would concern the "friendship requests" sent by other users.

Moreover, the photos and images in social platforms also represent another specific point to stress. Indeed, it would be desirable to have real possibility to avoid that other users (also “friends”) might post images of the other user without a preventive specific consent.

Last but not least, regarding the images/photos posted in the social platforms, it would be also desirable to have the technological pattern possibility not just to erase what already posted, but also to pre-assign a kind of expiration period of the photo posted (for example: posting a photo with a pre-set expiration period of 7 days; after the 7 days, the photo will disappear on the social platform). In addition and in connection with this, the possibility to pre-set that all photos posted cannot be downloaded by the other users would be also a very useful pattern in order to protect the rights of the users.

Marco Costantini

Data Protection Officer