**FREE TRASLATION**

**Facebook glasses: why so many doubts about compatibility with privacy rights**

In recent days EssilorLuxottica has presented to the public the Ray-Ban Stories smart glasses, made in collaboration with Facebook; the device, which has been released in some markets (including Italy), allows users to take photos and record videos with voice commands or by pressing a button on the right-hand spectacle rod. It also has small speakers that turn the smart glasses into headphones for listening to music and podcasts via Bluetooth from the smartphone they are paired with. And they include microphones so the users can also talk on the phone.

These glasses are "smart" because what the users record is stored on an app (from Facebook) and, later, if the users want, posted on the internet (hence the name "Stories", like the stories one posts on social networks).

What, therefore, makes this tool attractive (also given the fairly affordable cost), namely the possibility of passing with immediacy from the recording of reality to its entry on the web, is also what raises doubts about the compatibility of the smart glasses with the rights to privacy and which has also determined the intervention (albeit at the moment only in the form of a request for information) of the Italian Data Protection Authority.

The problem arises mainly from the fact that the smart glasses are associated with a smartphone app, Facebook View. After recording videos or taking photos, the content can be uploaded wirelessly to the app. Then, from Facebook View, the users can share the content in their social networks or messaging apps, as well as save the photos directly in their phones' memory on the device outside the Facebook View app.

Thus, all data, including images (and consequently biometric data) of third parties, even unwitting ones, taken by the users of the smart glasses are uploaded to the Facebook app. To protect – in theory – the privacy, a small indicator light comes on when the smart glasses are recording, alerting people who are being photographed or filmed. But, in the opinion of many, such indicator light is not so visible to a third party, it is only noticeable from very close up and, moreover, what tools could the third party who is being filmed against his/her will have?

According to the additional information that Facebook makes regarding the use of Facebook View, the company states that it collects, when using the app, "*Photo and video recordings*" (it explicitly states "*You can use the Glasses to take photos and record videos (with or without sound). You can then edit this content in the App. The content is stored in the Glasses until you upload it to the App. We also collect metadata about the content, such as the date and time it was created*"), and "*Device Information*", which is information that is collected through cookies, pixels and similar technologies, as well as device usage data (e.g. number of photos, time spent recording, length of videos recorded).

Explicit are the app's terms of use, which clearly state that the license granted to Facebook "*includes content that you share, post or upload to Facebook View or in connection with Facebook View. This implies, for example, that if you share, publish or upload videos using Facebook View, you give Facebook permission to store, copy and share them with other products of Facebook companies or services that support them*.".

What about the rights of third parties recorded or photographed by the users?

Guido Scorza, a member of the Italian Data Protection Authority, in an interview a few days ago rightly observed: "*When they take a photo and then publish it on social networks, they are sharing the personal data of the individuals who end up in the image, primarily their facial features. What worries me is the "careless" use of smart glasses by users who are not fully aware of the risks involved in sharing personal data online. Think of minors*".

According to the app's terms of use, Facebook states that "*You are responsible for complying with all applicable laws when using Facebook View, including providing notice to or obtaining consent from other individuals who use your Facebook View or interact with you while using it, as required under privacy or data protection laws or other applicable laws. You are also required to use Facebook View in a safe, lawful, and respectful manner.*".

This places the responsibility for any unlawful processing of third parties' personal data on the users of the smart glasses, who are not, however, obliged to comply with the GDPR. Indeed, the GDPR does not apply in the case of domestic use; recital 18 of the GDPR is explicit in this sense: "*This Regulation does not apply to the processing of personal data carried out by a natural person in the course of activities which are exclusively personal or domestic in nature and therefore not related to a commercial or professional activity. Activities of a personal or domestic nature could include correspondence and address books, or the use of social networks and online activities undertaken in the course of such activities.*".

Of course, the users using the smart glasses must still comply with the rules of Italian law, including article 10 of the Italian civil code (abuse of another person's image) and article 96 of the copyright act, and therefore, in theory, cannot film or even publish another individual's image without that individual's consent.

However, this protection is very limited, especially from a practical point of view.

Moreover, in many cases, not even the users of the smart glasses have the basic training to realize what is legitimate and what is not, to distinguish what is appropriate and respectful from what is not. We would also point out that the same conditions of use referred to above reserve the use of smart glasses and the associated app to persons over 13 years of age, an age at which there does not seem to be a sense of limitation and not even yet, unfortunately, sufficient education of the virtual world and the ways in which it should be used.

In conclusion, the same risk profiles highlighted by the European Data Protection Supervisor (EDPS) in its January 2019 report on smart glasses and data protection are highlighted, namely:

(i) the lack of control over the data collected, both by users and by individuals who come within the range of the smart glasses;
(ii) the intrusive and unauthorized analysis of the behavior of individuals;
(iii) the important limitations on the users' ability to remain anonymous;
(iv) the absolute lack of anonymity of the individuals who enter into the range of action of the smart glasses;
(v) the consequent processing also of special categories of data, which would instead require greater protection;
(vi) the greater risk deriving from the massive production and use of the smart glasses.

In fact, the Data Protection Authority asked the Irish Data Protection Commission (DPC) to ask Facebook to answer a number of questions. In particular, the Authority asked to know the legal basis on which Facebook processes personal data; the measures put in place to protect individuals occasionally filmed, in particular minors; any systems adopted to anonymize the data collected; and the features of the voice assistant connected to the smart glasses.

This was followed by two meetings, in which - the Authority states - Facebook and EssilorLuxottica "d*eclared their willingness to work, also in conjunction with the Authority, to launch information and awareness-raising initiatives with the aim of making both those who will buy the glasses and all citizens more responsible. The Authority reserves the right to assess the effectiveness of the operational proposals that will be presented by the companies.*".

Therefore, all that remains is to wait and see if smart glasses will be successful and widely used in our society (which has not happened with previous similar products launched on the market in recent years) and their concrete impact on the privacy of citizens, as well as to await developments in the work of the competent Authority.