media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 4/2016

**ALESSANDRO MONTI*** **- ELISA ROSATI****

# General Data Protection Regulation and Biometric Data

SUMMARY: 1. The Forthcoming General Data Protection Regulation (GDPR). - 2. The Need for Privacy Protection in the Context of Gathering Biometric Data. - 3. The Prospected Privacy Protection Improvements Provided by the Regulation. 4. The Protection of Biometric Data According to the Regulation. – 5. Conclusions.

## 1. *The Forthcoming General Data Protection Regulation (GDPR).*

After four years of waiting, it has happened.

On December 15th, 2015, the EU Commission, the Parliament, and the Council of Ministers agreed the final text of the General Data Protection Regulation ("GDPR" or "Regulation")[1]. The GDPR will be likely published in the EU Official Journal in the spring of

* PhD, Bocconi University – Lawyer at Santa Maria Studio Legale Associato

** Lawyer at Grimaldi Studio Legale

[1] On 25 January 2012, the EU Commission proposed a comprehensive data protection package comprising of: (i) proposal for a Directive on the protection of individuals with regard to the

2016. Once published, the rules would become official within a two-year span without the need for domestic implementing legislation. However, as better discussed below, the new Regulation does allow Member States to legislate on data protection matters.

There are no doubts the new Regulation will represent a major step forward in the implementation of the 'Digital Single Market Strategy'[2] but at this stage we can just predict the effectiveness in protecting our digital lifestyle.

The GDPR will have a huge impact on multinational companies doing business in the EU as it would introduce a new single data protection law they have to comply with. The new privacy framework designed by the legislator, which applies to all 28 European Member States, aims to harmonize data protection laws for entities that process personal data for EU residents. Theoretically, it is reasonable that a single set of rules on data protection valid across the EU may provide more consistency than different ones. Within a two-year span, we envisage that European companies have to adhere to stricter standards compared to companies established outside the EU but also doing business in the Single Market. With this reform companies based outside Europe will have to apply the same rules when they offer goods or services on the EU market.

It implies stepping from a connecting factor based on the establishment in EU or on the national territory[3] to the one based on the targeting of services and products for operators in the EU.

---

processing of personal data by competent authorities, which is intended to replace the "2008 Data Protection Framework Decision"; (ii) a proposal for a General Data Protection Regulation, whose text was confirmed last December 2015 by the Permanent Representatives Committee.

[2] Please, see: European Commission: Digital Single Market – Bringing down barriers to unlock online opportunities.

[3] Art. 4 (1) c, Directive No. 95/46.

2. *The Need for Privacy Protection in the Context of Gathering Biometric Data.*

The range of the new Regulation is even bigger if we consider the spread of any kind of mobile handsets (such as laptops, tablets and smartphones) in everyone's daily life. The beginning of the era of IoT (Internet-of-Things)[4] has opened new frontiers. In nearly everyone's daily routine, all smartphone users download and automatically update their mobile applications from app-stores available in the market to pay taxes, claim expenses, buy goods, and manage bank accounts – all online. There is little today that mobile technologies have not touched and transformed and the number is intended to increase in the close future. Evaluation says that by 2020, at least 26 billion devices will be hooked up to the internet; 70 percent of people will own a smartphone.

All these connected devices are hungry for data and they allow several log-in methods whether a simple password or more complex multi-factor authentication – combining the username (not necessarily confidential) with an exclusively confidential password. Modern systems use as a password alternatively either a PIN code, challenge question, or 'biometric data' such as a retinal/iris/fingerprint/facial, voice recognition.

In this scenario, the use of common apps such as: (1) social networks, instant messaging and VoIP/video calls, (2) GPS navigation mapping, (3) on-line shopping and loyalty card schemes has become more accessible. As a result, always more often companies are increasingly offering their own app to allow clients to enjoy the services directly through their devices. Most of these apps take advantage of the users' pastime and they may register information about him to process personalized and tailored offers based on customers'

[4] The initial use of the expression "Internet of Things" (IoT) has been attributed to Kevin Ashton, cofounder and executive director of the Auto-ID Center at MIT, who first mentioned it in a presentation he made to Procter & Gamble in 1999. It is a computing concept that defines the possibility to connect set of things to existing network and make them able to communicate to each other. In this way things would be adapt their behavior to data they receive by networks (i.e an alarm clock connected to a network and able to play in advance in case of traffic, or an intelligent mirror, or a home automation system that regulates temperature and lighting of the house depending either on the season or on the hour of the day).

behaviors and habits since the first use. Many of the applications available in the market need never more than a few clicks or taps away by data subject (individuals whose personal data is being processed) to allow data controllers (those responsible for the processing of data) to collect his/her "personal data". Sometimes, by giving easy flag one-click consent, any data subject often expressly authorizes the data controller to transfer and/or share its personal data to other EU-based companies of the same group or third-party services providers for marketing and promotional purposes.

Even the banks have decided to offer their customers app services that use biometric systems for security scopes. Examples are the online banks that allow the client to log in to his/her online account by recording his/her voice as password. Always in the banking sector, it is gathering momentum the implementation of behavioral anti-fraud systems which record, while the client browses the internet banking, the mouse movements (or the finger gesture in case of device touch) and the pressure on the screen with reference to the selection and speed of typing on the keyboard. Or in order to streamline the activity, others companies allow their employees to subscribe electronic documents with biometric techniques based on the detection of the writing a hand-written signature.

An effort to stop the lack of control was made by the authorities from around the world who had decided to sign an open letter[5] to the operators of seven app marketplaces (Apple, Google, Samsung, Microsoft, Nokia, BlackBerry and Amazon) urging them to make links to privacy policies mandatory for apps that collect personal information. It is aimed at all companies that operate apps in marketplaces. Given the wide-range and potential sensitivity of the data stored in mobile devices, the authorities believe that privacy practice information (for example, privacy policy links) should be required (and not optional) for apps that collect data in and through mobile devices within an app marketplace store. Authorities stressed

[5] Global Privacy Enforcement Network (GPEN) asked the platforms offering apps on smartphones and tablets to oblige developers to notify users before they discharge apps, on any personal data that will be collected and their use (Joint Open Letter to App Marketplaces, December 9, 2014).

that Individuals need to be meaningfully informed regarding the collection and use of their data before making the decision to download the app.

But the question is: honestly, how many of you have read the information on data protection before downloading an app?

3. *The Prospected Privacy Protection Improvements Provided by the Regulation.*

The Regulation intends to increase the protection of individuals by strengthening their existing rights and guaranteeing a greater control over their data (through the easy access to personal data, the need for clear individual's consent for processing his or her personal data, his/her right to object and also with regard to the use of his/her personal data for the purposes of profiling) on the one hand and by setting additional burdens for data controllers on the other.

Data controllers will be required to provide better information to data subject on what happens to personal data once it is shared. This will include informing individuals about their privacy policy in clear and plain language, which can also be done via standardized icons. Information on data may be provided with explanatory sketches to make the data subject more aware. Moreover, the Regulation will place onerous accountability obligations on data controller who will have to set from the beginning all measures required to be compliant with data protection laws. It is time for businesses to figure a plan out to demonstrate compliance and the adoption of appropriate measures able to guarantee quickly notification in case of personal data breaches. When the processing uses new technologies, and in consideration of the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, the controller shall be burdened to carry out a data protection impact assessment (DPIA) prior to the processing of personal data in order to assess the particular likelihood and severity of the high risk.

In addition, those companies cause of performing certain risky data processing, particularly those that handle sensitive data like biometrics or health information, have to designate a data protection officer (a DPO), to ensure compliance with the rules.

Another interesting and connected concept set out in the Regulation is privacy by design[6] requiring that data protection safeguards must be built into products and services from the earliest stage of development. A concept entered in the Italian System thanks to Article 3 of the Decree No. 196/2003 ("Privacy Code") entitled "Principle of necessity in data processing". According to this principle, the ICT systems and programs should be set in order to minimize the use of personal data, and at least avoid the processing when the purpose can be however achieved by using either anonymous data or mechanisms that identify the subject only in case of need. According to this setting, the user is considered the center of the privacy system. Any project has to be figured out since the beginning to be designed (indeed by design) to grant protection of personal data.

Particular attention is also given to children. Companies will have to guarantee the removal without delay of personal data collected or published on a social network when the individual is still a child. The human being is assuming a central position in the data privacy system and businesses have to adapt to this. It will likely be a long process that calls on companies interested in doing business in Europe a commitment in terms of time and cost, but we like to believe that it will bring advantages in the new technological era.

[6] The concept of Privacy by Design (PbD) is not new. It was already known and used in the United States and Canada, and it has been recognized in 2010 at the 32nd World Conference of Privacy Commissioners who adopted the resolution on Privacy by Design, thereby making it official.

4. *The Protection of Biometric Data According to the Regulation.*

According to the definition of 'biometric data'[7] provided by the drafted Regulation, we should not have any doubt that biometric data are personal data insofar they allow or confirm the unique identification of a data subject.

However, thanks to the continuous development, new hardware technologies are going to be implemented to allow the collection in an anonymous aggregated form of certain raw physiological, morphological and behavioral characteristics belonging to individuals. Such hardware technologies may be used, also combined with software apps, to process statistics, for example, related to internet connectivity and data coverage or customer profiling in stores (people counting, recognition of gender, ethnicity, age group, *etc.*).

In the light of the above, we wonder 'if' and 'what' kind of protection should be granted to individuals whose biometric data are collected anonymously.

In this regard, it should be noted that biometric data are included in those types of processing that according to the Regulation might require a DPIA (data protection impact assessment). Moreover, the Regulation leaves large margins of action to the national legislator, who is allowed to provide for additional conditions or limitations with regard to certain data types, including those pertaining to biometrics.

5. *Conclusions*.

It may be inferred from the above that is definitively too early to make final judgments on the protection of biometric data and, more broadly, of personal data.

[7] "Biometric data means any personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data" (Article 4, paragraph 11).

Our hope is the autonomy granted to the national authorities lead to advantages and not to limit for the completion of the harmonization process. Member States would carry on their activities, keeping in mind the principles behind the privacy system. As Andrus Ansip[8] said: "(…) The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information. And they can enjoy all the services and opportunities of a digital single market. We should not see privacy and data protection as holding back economics activities. They are in fact an essential competitive advantage. (…) Our next step is now to remove unjustified barriers which limit cross- border data flow (…). So let us move ahead and build an open and thriving data economy in the EU- based on highest data protection standards and without unjustified barriers."

On the other hand, in the view to a greater efficiency of the System and to provide certainty in the privacy sector in case of disputes, the Regulation should provide that companies active in several Member States will deal only with the data protection authority where its main establishment[9] is located. In this way, since businesses will only have to deal with one single supervisory authority ('one stop shop mechanism'), we cannot exclude that multi-national companies may be influenced by the future national provisions to choose their main establishment.

[8] Vice president for the Digital Single Market, Brussels, 15 December 2015.

[9] If you want to know more on how the EU arrived at the current position in relation to the One Stop Shop, please look at the following:
a) the position under the Commission proposal for the new Regulation in 2012 (Commission 2012 Proposal);
b) the most significant differences between the Commission 2012 Proposal and the Parliament's adopted text of 12 March 2014 (Parliament March 2014 Position); and
c) the Council's latest internal compromise position: the 'Partial Agreement' on this aspect of the Regulation reached among its members on 13 March 2015 (Council March 2015 Position).