# FROM DATA PROTECTION TO «PRIVACY BY RESEARCH» FOOD FOR THOUGHT IN THE LIGHT OF THE NEW EUROPEAN GENERAL DATA PROTECTION REGULATION

***Simone Calzolaio****
***Valentina Pagnanelli*****

*The paper recalls the process which led to the adoption of the new european Data Protection Regulation, in the context of the rapid development of the Information and Communication Technologies and the amazing increase of data flows (Big data). Data Protection and Privacy Protection could be seen as limits to the development of technologies. On the other hand, the rapid evolution of Smart cities and ICTs brings new risks for the protection of fundamental rights. The new european Regulation n. 2016/679 could be insufficient to protect privacy rights in the age of Big data. Maybe some new instrument is necessary to protect personal data and, consequently, privacy. The paper proposes the concept of «Privacy by Research», intended as a new privacy-friendly method of design for devices, databases and apps.*

*Albeit its unitary conception, Simone Calzolaio drafted Sections 1, 2, 3 while Valentina Pagnanelli drafted Sections 4 and 5.*

## 1. DIFFERENT POINTS OF VIEW ON PRIVACY AND THE INTERNET. PRIVACY AS A LIMIT TO EVOLUTION OR A WORTH PRESERVING VALUE?

Computer scientists and law scholars normally observe the evolution of the Internet from two different points of view.

The first ones act like pioneers in search of new technological discoveries; they do not worry much about the endless accumulation of data (and personal data).

The second ones, conversely, tend to see problems everywhere: it is no coincidence that many publications on data protection contain the word "threat".

The consequence is a clear distinction between two ways of observing the evolution of the Internet.

On the one hand there are those who see threats to privacy [5, Rodota, 1995], and on the other hand there are those who feel threatened by privacy protection, because of the risk that data protection could end up restricting the freedom of the Internet [4, Poullet, 2009].

This difference of views, as well as a substantial number of practical problems, is strongly influencing the way in which law experts intend to act in the field of privacy protection.

To get good privacy regulations it would probably be advisable to abandon the dispute between cyberlibertarians and cyberpaternalists (Bernal, 2014).

Anyway, it is a matter of fact that the rapid development of the Information and Communication Society has taken to a reality where *"The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy* (1)".

* **Simone Calzolaio**, Researcher of Constitutional Law at the University of Macerata, Italy.
** **Valentina Pagnanelli**, lawyer in Macerata, Italy.

It's worth mentioning three cases related with the growth of ICT that can be seen as innovations and also as threats to privacy: the Internet of Things (IOT), the practices of Profiling and Behavioral Tracking, and the increasing Cross-border data Flows.

First, the so-called IOT: even if the definition is not universally shared, it can be said that IOT is the use of things through the Internet by man. IOT is the connection of everyday objects (eg TV, appliences and exercise equipments) to the Internet [3, p. 99]. Actually this innovation enables to collect a big amount of data about property, people, plants, animals [3, p.99].

Many aspects of life can be managed simply using a smart phone. This is a consistent innovation but at the same time it involves risks.

Security systems for data handled through IOT are not yet adequate. For example hackers could easily reach all the data (and consequently information) relating to the users, and use them for blackmail activities or to commit other crimes.

That particular kind of data mining called Profilation is another potentially dangerous activity.

*"Profiling is a technique of (partly) automated processing of personal and/or non-personal data, aimed at producing knowledge by inferring correlations from data in the form of profiles that can subsequently be applied as a basis for decision-making.*

*A profile is a set of correlated data that represents a (individual or collective) subject.*

*Constructing profiles is the process of discovering unknown patterns between data in large sets that can be used to create profiles.*

*Applying profiles is the process of identifying and representing a specific individual or group as fitting a profile and of taking some form of decision based on this identification and representation".* [1, p. 3]

Profiling could be considered a threat to privacy because of the amount of data handled and collected by the data processors and because of the private or governmental use of the results obtained (2).

The Directive 95/46/EC on privacy doesn't mention the word "profilation", even if there is a provision about activities related to profilation. The new european Regulation conversely contains a more specific provision about profiling techniques with the enunciation of stricter rules (3), but nevertheless the use of profilation is considered to be a risky pratice for the protection of privacy, as we shall see in the following parts of this paper.

Also the so-called Behavioral Tracking is strictly connected with smart technologies. This practice is based on cookies, that are useful to get information about life-style, interests and buying habits of individuals.

On-line tracking has enhanced the potential of off-line profiling; nowadays the on-line tracking, together with the volountary submission of personal information through the social networks (4), allows companies to collect a big amount of personal information of impressive commercial and economic value [6, p.35].

Third case, the cross-border data flows represent another example of potential data protection risk: it is still a priority for Goverments and Regional and International Institutions to ensure safety and privacy of data transmitted from a State to another, expecially if out of european borders.

Safe cross-border data flows are needed to develop the single market, and also to ensure international trade, but the security of those flows is not always adequate, and legislation need to be updated. Generally speaking, data protection rules should not interfere with business, but the market should not use personal data as "goods without owners (5)".

These examples seem to confirm the need to develop at least two additional fields of investigation and search for law scholars and computer scientists: Privacy Protection as an independent object of research and Privacy Protection as technological standard of research in progress.

## 2. THE SURFING IN THE INTERNET AND THE WAY BACK TO THE RIGHT TO BE LET ALONE

As highlighted above, the use of new technologies like email, social networks, on-line banking, GPS navigation system, video games, apps, public wi-fi and so on, makes people produce an avalanche of data.

Consequently, nowadays almost all law studies collect and list the actual risks associated with the evolution of the use of the Internet. Whether if we see it as an opportunity or as a risk, it is a matter of fact that the amount of data associated with us is increasing steadly. With the so-called *Smart cities* it is no longer to share information or services through the Internet, but to manage the things we do, and we use in our private life or in our personal businesses (6).

Normally it comes to personal data. Often it comes to sensitive data.

It is true that all the apps and services that people usually use could not exist without a constant data flow.

On the other hand, the set of data related to each person could somehow jeopardize the

so-called Habeas data (that is, the right to protection of personal data and the so-called right to informational self-determination (7)), with considerable impact on private life.

Today you can get very personal information (sensitive information) about any person just by crossing simple and/or personal data. This is the so-called "Big data": a huge amount of data, produced daily because of the digital lives of people, companies, governments, and then handled and stored in those non-places called "clouds (8)". This data, properly interrogated, becomes a source of endless information, with a great economic value. The result is a new and flourishing field of research: the "Big data analytics." Currently, it is no longer necessary to process personal or sensitive data, to draw analytical information on individuals.

Only by querying and crossing Big data (date inference and re-identification) it is possible to obtain personal, analytical, intimate, confidential information (9). It is interesting to note, therefore, how the technological evolution and the impact of the digital life on the real life is gradually making obsolete what only a few years ago was an acute innovation. Article 7 (on the right to respect for private and family life) and Article 8 (on the right to the protection of personal data) of the EU Charter of Fundamental Rights distinguish two rights that are probably one (10). In the case of the so-called Digital natives, data protection and protection of private and family life tend to coincide since their birth. Nowadays it seems almost impossible to defend our right to be let alone, as a right to withdraw from society (11); citizens seem to be able to defend at least their "right to be forgotten", which is a the renewed version of the right to privacy [8, Warren & Brandeis, 1890], connected to our digital life. Our privacy seems to coincide with our digital life, and as we said, privacy tends to become one with data protection.

Already before the adoption of the new Regulation, the European Court of Justice (ECJ) ruled on the fundamental right to privacy. In the famous Google Spain judgement (12), the ECJ proclaimed the existence of the just mentioned right to be forgotten, with and extensive interpretation of the provisions of Directive 95/46. The decision focused on the lack of a specific provision in the existing european set of rules, de facto highlighting the need for the european legislator to fill the gap (13). Today, Article 17 of the General Data Protection Regulation (GDPR) states the existence of a Right to Erasure (Right to be forgotten), which seems to be nothing but a personal data management tool, useful to protect private life, through data protection. The European Court of Justice has had the role of defender of personal data, in another important decision, the so called Facebook case, in which the judges of Luxembourg declared the invalidity of the Safe Harbour scheme, containing the fundamental principles about transfers of personal data from the European Union to United States (14). The decision states that "*the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments* (15)", and therefore the data transfers from EU to US had to be considered at risk for data security. As a result of the Facebook decision, the Safe Harbour framework has been quickly replaced by the new EU-US Privacy Shield Framework (16). On 12/07/2016 the European Commission adopted its decision on the EU-US Privacy Shield, which allegedly contains more obligations for companies, guarantees for citizens, greater transparency in data processing and controls, as well as mode coded complaint. The possibility remains for the US Intelligence to get hold of personal data for security purposes, but with certain limitations. Only a trial period will allow to make assessments on the effectiveness of the new agreement. What is important to note is that the Court, by protecting in different ways the personal data of european citizens, has created a kind of "european personal data", which need to be protected because of its economic value, and because of the real risk for privacy of persons.

It is therefore easy to see that the evolution of the european legal framework on data protection was already in progress at the moment of the adoption of Data Protection Package. But it is certainly the GDPR that takes a very important step forward effectiveness of data protection, by defining and regulating profiling in several provisions (17).

Actually the previously mentioned technique of profiling is a perfect exemple of union between personal data and privacy – and plastically between Articles 7 and 8 of the Charter - and at the same time of the high risk associated with this technique. Profilation is a risky practice because the data subject could lose his/her right not to be subjected to a decision, which is based solely on automated processing of personal information and which produces legal effects concerning him/her, such as the automatic refusal of an application for online credit or electronic hiring practices without human intervention.

The two cases described above, together with the new European legislation on profila-

tion, show the huge importance of the control on personal data, that is an effective protection of privacy, and which is closely linked to the increase of the use of digital services.

**3. A DEEPER LOOK ON WHAT A SENSITIVE DATA IS TODAY (AND THE NEW EUROPEAN WAY TO PROTECT PRIVACY)**

As just said above, the evolution of the Internet makes us reflect on what is a personal data and, in particular, a sensitive data.

By itself the sensitive data is the personal data suitable to reveal the racial and ethnic origin, religious or philosophical beliefs, political opinions, trade-union membership, as well as the personal data suitable for disclosing health or sex life (18).

The difference between the personal and sensitive data is that the personal information allows or may allow the identification of data subject, while the sensitive data allows or may allow the identification of the personality of data subject.

However, the evolution of the Internet suggests that it is not easy and may not be sufficient to define abstractly what a sensitive data is.

For example, a multiplicity of personal data process do not produce - in European Directive 95/46 – a single sensitive data. None of them - normally - is a sensitive data.

Anyway, as already seen on paragraph 2, a simple set of (not personal) data referring generically to a certain environment which are crossed with another set of personal data are certainly allowing the disclosure of racial or ethnic origin, religious, philosophical and political beliefs, health status and sexual life of a person much more than a set of sensitive data.

The amazing growth of the use of the Internet produces huge quantities of data. From these data, often merely generic or personal, it is easy to obtain sensitive or highly sensitive data about people.

Therefore, "sensitive data" is not conditional only to the nature and to the character of the data, but are also involved with the amount of general and personal data available in the Internet. Sensitive data is something dynamic, related to the procedures and practices of Internet use, as much as to the nature and character of the data.

And indeed the new european Regulation takes into account this new context in which all data can give sensitive information if correctly crossed and combined with other data. The GDPR gives to Member States the opportunity to choose the way to protect special categories of data (sensitive data (19)), recognizing the need for Member States to assess wheter a processing of data leads to a revelation of personal information or not.

Even if Article 9 recalls the former statements about sensitive data, the real regulation is in Article 4. There we find new definitions, that better fit on the emergence of new risks for personal data (and privacy). In this context the reason for the introduction of definitions such "profilation (20)" and "'pseudonymisation (21)" seems clearer. The new european legislation has taken note of the profound change in conditions, primariliy due to the evolution of technologies. On the one side it sharpens the set of definitions about types of data and types of processess. On the other side it leaves a consistent "margin of manoeuvre" to Member States, to specify their rules for particular kind of informations.

But before going on with this reflection it shall be useful to have a look at a worldwide perspective about use of data and ICT. It will help to understand the reasons of such political and legislative strategies of the European Union.

**4. A WORLDWIDE PERSPECTIVE. THE BIRTH OF "EUROPEAN PERSONAL DATA"?**

If we look at the trend of data production, data processing and data retention on a map, we can easily observe that there are three major global players, playing different roles and having different rules on data protection.

Most of technological devices used to surf in the Web (personal computers, smartphones and so on) are produced in Asia and, in particular, in China. Nevertheless China is shielded from information and data flows coming from abroad, but it not committed to defending the privacy of chinese citizens.

The United States instead produces most of the necessary tools to surf in the Interet (and consequently to create Big Data): apps, Internet services as cloud computing, video games and so on. The US is the country where most of the data are collected and stored.

It is interesting to note that the United States does not have a general data protection law. However, it's no surprise that US has a legislation on Intellectual Property and protection of economic exploitation of softwares (22).

The European Union in this context plays a special role. It does not produce devices and is a not-so-big producer of services for the Internet. However, european citizens are the biggest consumers of devices and at the same time the biggest data producers in the world.

The European Union is the major producer of data, the ones we called "european personal data"; most of this european data ends up in the United States.

It is no coincidence, then, that the European Union data protection system is more restrictive than in the United States and China.

Let's briefly recall the european model of strict-regulation, and the opposite model of US self-regulation (23).

The continental model is based on a very pervasive set of rules, that try to govern all the aspects of the internet and the relationships trought the different actors of the economic scene (OTT, providers, devices producers, customers...). Strict-regulation corresponds to the presence of many sources of law, many rules from different institutions, and also to the creation of specialised, independent authorities.

The US model on the other hand is based on the idea that in some ways technology can rule by itself.

"Self-regulation" corresponds to a substantial absence of public institutions in the creation and impleementation of standards: the main actors shall be the ICT-companies and other stakeholders. This system is supposed to ensure a better protection of the activities on the Internet: control on contents, protection of personal data, protection of Intellectual Property rights (24).

Conversely, in the just described context of roles and relations, the European Union goes on on the path of strict-regulation, choosing to substitute a Directive with a Regulation on data protection. Many scholars seem to be doubtful about this choise, as we shall see.

**5. THE STRANGE ROLE OF THE EUROPEAN UNION.**

***5.1 The path from the Directive to the General Regulation***

The fast and irrepressible evolution of the information society, together with globalization and increasing digitization of human activities (e-commerce, e-government, e-health ...) have gradually revealed the inadequacy of 1995's law to cope with the digital and telematic transposition of traditional and new digital native cases.

The growing need to protect all these legal situations, joined to the strategic importance of the management and use of personal data in the development of the Digital Single Market, have been the engine of decisive legislative steps.

It is no coincidence that the power to regulate data protection has become - since the Treaty of Lisbon - a competence of the EU. And thus, the new EU Regulation on data protection n. 2016/679, repealing Directive 95/46/EC which regulated the protection of personal data in the EU over the last twenty years, seems to indicate a clear change of pace of European Union.

Indeed the European Union has the stated purpose to get *"the highest data protection standards in the world* (25)" to generate trust in the consumers and to accelerate and enhance the economic growth of the Digital Single Market. The adoption of the GDPR seems to confirm this aim.

Let's briefly recall the main difference between Directives and Regulations. The first ones leave Member States the power to implement the Directive through national legislation and, accordingly, the possibility of introducing significant variations in the regulation of specific aspects of national law. Instead, a Regulation is directly applicable throughout the EU and it does not need another Member state law to be applied (26).

The Directive 95/46 had equipped the then Community of a first European "model" of protection of personal data, with a matrix containing all the essential elements to afford the national data protection tools (definitions, regulations, establishment of a supervisory authority, sanctions, rules for special sectors). This scheme was then also significantly declined in different ways by Member States, in the transposition phase. Indeed Recent studies show that each European country applied the Privacy Directive very differently.

The GDPR n. 2016/679 is now supposed to ensure a uniform application of the rules on data protection (27).

As it has been said previously, the approval of the Data Protection Regulation was anticipated and in some way suggested by the activity of the European Court of Justice.

The mentioned decisions Google Spain (on the right to and responsibility for the search engine), Facebook (on the transfer of personal data to the United States) and the one about Data Retention (with declaration of invalidity of Directive 2006/24 (28)), have drawn attention on matters of crucial importance, on which later European legislator intervened [2, p.681].

So, the new Data Protection Package, together with the Roaming Directive (29), as well as that of 2013 on Re-use of Public Sector Data (30) now introduce in the European Union many instances of renewal, focusing attention on IT evolution, and placing the information society in the core of the Digital Single Market, the heart of the European Union.

***5.2 Contents of the Regulation***

The Regulation 2016/679 confirms the general principles of data protection, and introduces important new features.

As just mentioned, the innovations included in the Regulation were needed, given the prodigious development of the Information Society, and thus given the need to provide the EU with a unitary set of rules.

The guarantee of a single body of law uniformly applicable in the whole European Union will hopefully enhance the protection of personal data of citizens, and it is also supposed to accelerate and simplify the development of businesses.

Firstly the reform should lighten the bureaucracy, by reducing notification requirements. Another important step towards simplification should be the so called one-stop-shop system: a company operating in different States will only have to deal with one Data Protection Authority (DPA), that is the Authority of the Country where the company has its principal base (Art. 56).

Moreover, the new GDPR will apply also to extra-european companies offering products and services to european citizens (Art. 3), in this way trying to solve the huge problem of jurisdiction and applicable law to companies operating with ICT.

On the other hand, the new Regulation has te objective of strengthening the protection of fundamental rights of citizens.

It's the case of the many times mentioned right to be forgotten, at first theorized and protected by the Court of Justice, and now canonized in Art. 17, in a statement which takes into account the necessary balance between privacy and freedom of information.

The Regulation also introduces and formalizes the existing principle of Privacy by design. Actually a reference to Privacy by Design was already contained in the forty-sixth Considering the 1995 Directive (31), but it had not been transposed among the provisions of the act.

Furthermore, this rule was already part of the proposals for the review of the Convention n. 108 of the Council of Europe for the Protection of Individuals with Regard to the Processing of Personal Data (32), submitted in 2012 by the Consultative Committee (33).

Today the "Data protection by Design (and by Default)" is a general principle of privacy-friendly setting of products and services, regulated by Art. 25 of the new General Regulation.

The new Regulation introduces many other important rules.

Here is a quick mention of the main of them.

First of all, the data portability: it ensures that the transmission of personal data of a data subject from a controller to another takes place without obstacles (34).

The new rules also impose to organizations and companies to notify to the data subject and to the data protection authority if data is accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons (35) (Data breaches, Art. 33-34).

The new GDPR should also increase responsibility and accountability for the controller and the processor, with the introduction of the data protection impact assessment and the introduction of the figure of the data protection officer (36) (Artt. 35 ff.).

Finally, the new GDPR reveals a greater awareness than in 1995 of the economic value of personal data and of the great risks that lie behind the processing of Big Data which characterizes the Information and Communication Society (37).

***5.3 Limits of the Regulation and limits of law. The need of a «Privacy by research».***

Many scholars analyzing the Regulation highlighted numerous critical flaws.

In the legal world it is now widely believed that the traditional principles governing data protection are no longer adequate to manage the communication and information through the Internet.

The reaction of the jurist - as can be seen also in the Regulation n. 2016/679 - is to introduce new laws.

But someone says that the new set of rules risks to be already outdated at the moment it will entry into force (38).

First, this Regulation will be effective from 2018, and the intervention of the Member States in the implementation phase will be sensitive. The timescale necessary for Member States to comply with the new law seems to be really extended, in comparison to the speed of change of technological development. There is the real risk for the new GDPR to be already obsolete once it comes into force. Large companies and stakeholders on the other hand will enjoy a good amount of time to deal with the new rules and possibly overcome them.

Second, the regulatory model adopted by the european legislator seems to be, once again, anchored to a traditional idea of privacy law, where rules are addressed to the controller and data protection does not empowers the data subjects (39).

Moreover, the new european Regulation, being a stiff instrument, risks not to be updated with respect to the continuous changes of technology (and Digital Market): with the GDPR the gap between law in the books and reality seems to increase rather than decrease (40).

Even singular instruments regulated by the GDPR seem to be not-so-effective.

For example, it is worth asking wheter forms of impact assessment of privacy (privacy by design) and self-management of data (privacy by default) will be effective or not.

In other words, we have to wonder if the new privacy impact assessment is enough to achieve the purpose of an effective guarantee of data protection or it is just a bureaucratic exercise more. From many parts it has been suggested to better protect privacy by strenghtening *habeas data*, which is the real control of our data, by creating new instruments and somehow overcoming the consent as the main tool to control personal data (41).

Privacy by design could be the right instrument, because of its very nature, and it could drive institutions and actors of the IC Society to move *from a reactive to a proactive approach to privacy* [7, p. 331].

But maybe it is not enough, because data protection is not in the hands of data subjects. A new instrument is needed, through which the person shall be the owner of his/her data, and he or she will be able to decide about the use of it.

So, a new way of thinking is needed. One option could be a contractual approach which is centred on the agreement of the parties on the use of personal data (42); otherwise it is necessary to introduce a flexible tool (43), not linked with stringent provisions, and focused on a prior understanding and prediction of the risks connected to the loss of the sovereignity of the people over their data. This new tool shall be useful to create a technological environment in which the data subject will be the real controller of his/her own data.

Privacy by Research shall be a new method of design for databases, apps and devices. The starting point is a quite different assumpion from the previous ideas of Privacy by Design and by Default. Actually, Privacy by Design and by Default endow the data subject of a device where the data protection-settings are already set (even if they're privacy-friendly). The new proposed method allows people to keep control of their own data and to decide case by case whether to consent to a specific processing or not, and whether to consent to data tranfers, especially when cross-boarder, or not.

Therefore, the transition from Privacy by Design to Privacy by Research shall ensure better protection of the right to privacy, through the obligation to create goods and services which leave to the users the freedom to decide, before each processing, the fate of their own data. This possibility of greater control over every processing of data, shall eventually give the opportunity for the revival of the *habeas data*, intended as a complete and effective informational self-determination.

In conclusion, even after the approval of the new european legislation, it is clear that an effective protection of personal data is tightly linked to the close alliance of computer scientists and jurists. Indeed, it is true that the effective protection of personal data should be stricly connected to a rigorous treatment planning (privacy by design). But it is especially true that no effective treatment planning is feasible without a digital infrastructure created just to enable effective protection of personal data («privacy by reasearch»).

**Notes**

1. E-privacy Directive 2002/58/EC, Whereas no. 6. Significantly the new european Data Protection Regulation n. 2016/679/2016 contains specific references to the concept of risk; see Whereas no. 75, Art. 35. About the links between data protection and the notion of risk, see GELLERT R., *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative,* in International Data Privacy Law, 2015, Vol.. 5 No. 1.

2. See D'ALFONSO S., *Tutela dei diritti e Governance della rete,* ARACNE Editrice S.r.l., 2012, p. 38 on the project of the Center for Collective Intelligence of Massachusetts Institute of Technology (MIT), in particular about the need of a balance between social benefits and contra legem use of personal data.

3. See Whereas n. 71: "*The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it*

*produces legal effects concerning him or her or similarly significantly affects him or her.*"

4. See Regulation 2016/679/UE, Art. 9, lett. e): it is allowed to process sensitive data when they are manifestly made public by the data subject.

5. And data subjects as "*mere objects*", POULLET Y., op. cit. p. 215.

6. About Ubiquitous computing and Ambient intelligence technologies, see POULLET Y., op. cit. p. 221.

7. See RODOTÀ S., *La "privacy" tra individuo e collettività, in Politica del diritto,* 1974; RODOTÀ S., *Persona,riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali,* in Rivista critica del diritto privato,1997; CERRI A., *Riservatezza (diritto alla)*, Diritto costituzionale, in Enciclopedia giuridica, vol. XXVIII, Roma,Treccani, 1995; BUSIA G., *«Riservatezza (diritto alla)»*, in Digesto/pubbl., Agg., Torino, 2000, 481. DE SIERVO U., *Tutela dei dati personali e riservatezza,* in AA. VV., Diritti, nuove tecnologie, trasformazioni sociali: scritti in memoriadi Paolo Barile, Padova, Cedam, 2003; SALERNO G.M., *La protezione della riservatezza e l'inviolabilità della corrispondenza,* in RIDOLA P., NANIA R. (a cura di), I diritti costituzionali, Giappichelli, Torino, 2006, vol. II, pp. 617ss.

8. "Nothing in the last two thousand years has brought more fun to international law than the introduction of the Internet. There are cuontless entertaining legal situations arising of the fact that information can move across jurisdictions with no costs, efforts, or even without anybody really noticing – not to mention the fact that with latest cloud technologies, it is becoming impossible to physically locate or localise information at all", POLCAK R., Gettin European data protection off the ground, in International Data Privacy Law, 2014, Vol, 4 No. 4, p. 285-286.

9. A complete explanation of the phenomenon and the technical possibilities to combine it with data protection in D'ACQUISTO G., DOMINGO-FERRER J., KIKIRAS P., TORRA V., YA DE MONTJOYE, BOURKA A., *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics,* European Union Agency for network and information security, december 2015, in <http://www.enisa.europa.eu>.

10. On the Charter of Fundamental Rights of European Union see BIFULCO R., CARTABIA M., CELOTTO A. (a cura di), *L'Europa dei diritti: commento alla Carta dei diritti fondamentali dell'Unione europea,* Il Mulino, Bologna, 2001; GONZÁLEZ FUSTER G., *The Emergence of Personal Data Protection as a Fundamental Right of the UE, Law, Governance and Technology Series, Springer, 2014, p. 163 ff.*

11. "*Our walls no longer hide us*", POULLET Y., op. cit., p. 213-214.

12. Court of Justice of the European Union, C 131/12, 13/05/2014 http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 ; See PIZZETTI F., *Le Autorità garanti per la protezione dei dati personali e la sentenzadella Corte di giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya", in Diritto dell'informazione edell'informatica, 2014, pp. 805 ss.;* POLLICINO O., *Un digital right to privacy preso (troppo) sul serio dai giudici diLussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain, in Diritto dell'informazionee dell'informatica, 2014, pp. 569 ss. ;* FINOCCHIARO G., *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems, in Diritto dell'informazione e dell'informatica, 2015, p. 779;* VAN ALSENOY B., KOEKKOEK M., *Internet snd jurisdiction after Google Spain: the extraterritorial reach of the "right to be delisted",* in International Data Privacy Law 2015, Vol. 5 No. 2.

13. See MARKOU C., The 'Right to be Forgotten': Ten Reasons Why It Should Be Forgotten, in *Law, Governance and Technology Series, Reforming European Data Protection Law,* Vol. 20, Gutwirth – Leenes – de Hert Editors, Springer, 2015.

14. Court of Justice of the European Union, C 362/14, 6/10/2015 http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en .

15. Ibidem, n. 97.

16. "*The EU-U.S. Privacy Shield Framework was designed by the US Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce",* https://www.privacyshield.gov/welcome .

17. See Whereas n. 71 and Art. 22.

18. See Directive 95/46/CE Art. 8, GDPR, Art. 9, and also Convention n. 108, Art. 6.

19. "*In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data')*", Whereas n. 10, GDPR.

20. See supra paragraph 2.

21. *"The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".*

22. On the contraposition between "TLC-centric" system and "OTT-centric" system see D'ALFONSO S., op. cit., pp. 71-72.

23. See D'ALFONSO S., supra, p. 85 ff.

24. Ibidem.

25. http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf

26. Even if the GDPR leaves large margin of manouvre to Member States; see par. 3.

27. See PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino, Giappichelli, 2016.

28. Court of Justice of the European Union, C 293/12 – C 594/12, 8/04/2014 http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1018385

29. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=IT

30. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0037&from=IT

31. *"Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected".*

32. Avaible at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 .

33. Avaible at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_E_Convention%20108%20modernised%20version.pdf .

34. Regulation 2016/679, Art. 20, Right to data portability - *"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided [...]".*

35. http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf.

36. This figure, which raises doubts on its independence and neutrality, will be designated by the controller and the processor, and will be involved in all matters relating to data protection. The data protection officer will give advice, will monitor the correct application of the Regulation, act as contact with the Control Authority. The data protection officer will be in contact with the DPA. It will operate both in private and in public enterprises as well as in public bodies and authorities.

37. This new awareness can be seen also in the renewed list of definitions (Art. 4): to the ones already contained in the Directive 95/46 are now added those of "profiling", "pseudonymisation", "recipient", "main establishment" and others.

38. Among others. ERDOS D., *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gap,* in Legal Studies Research, Paper Series, Paper n. 30/2015, May 2015, University of Cambridge, Faculty of Law, pp. 19-20; KROOPS B.J., *The Trouble with European data protection law,* in International Data Privacy Law, 2014, Vol. 4, no. 4, p. 250: *"The trouble with the law, as with Hitchcock's Harry, is that is dead. What the statues describe and how the courts interpret this has usually only a marginal effect on data-processing practices. Data protection law is a dead letter; current ideas what to do with the body are not leading anywhere except that they offer entertainment to specators. With the current reform, the letter of data protection law will remail stone-dead".*

39. See BLUME P., *The myths pertaining to the proposed General Data Protection Regulation,* in International Data Privacy Law, 2014, Vol. 4, No. 4.

40. *"The on-going focus on command-and-control regulation to the neglect of other regulatory tools does not help either to achieve better data protection in practice",* KROOPS B.J., op. cit. p. 256.

41. About the effectiveness of consent see among others: POULLET Y., op. cit., KROOPS B.J., op. cit., BLUME P., op. cit.

42. POULLET Y., op. cit., p. 225.

43. POLCAK R., op. cit., p. 289.

**References:**


1. Bosco F., Creemers N., Ferraris V., Guagnin D., Koops B-J, (2015) *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities,* in S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law,* Law, Governance and Technology Series, vol. 20, Springer.
2. Mantelero A., (2014), *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella digital economy* [The future EU regulation on personal data and the "political" significance of the Google case: remembering and forgetting in the digital economy] // Diritto dell'informazione e dell'informatica [Information and Information Science Law].
3. Maras M-H, (2015) *Internet of things: security and privacy implications* // International Data Privacy Law, Vol. 5. No. 2.
4. Poullet Y. (2009), *Data protection legislation: What is at stake for our society and democracy?* // Computer Law and Security Review: The International Journal of Technology and Practice. Vol. 25. Issue 3.
5. Rodotà S., (1995), *Tecnologie e diritti* [Technologies and Rights]. Bologna, Il Mulino
6. Skouma G., Léonard L., (2015) On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law,* Law, Governance and Technology Series, vol. 20, Springer.
7. Von Dietze A., Allgrove A.M., (2014) *Australian privacy reforms – an overhauled data protection regime for Australia* // International Data Privacy Law. 2014. Vol. 4. No. 4.
8. Warren S., Brandeis L., (1890) *The right to privacy* // Harward Law Review. Vol. IV. December 15, 1890. No. 5.
9. Aparicio Salom J., (2014) *«A third party to whom data are disclosed»: A third group among those processing data* // International Data Privacy Law. Vol. 4. No. 3.
10. Austin L.M, (2015) *Enough about me: why privacy is about power, not consent (or harm)* // A. Sarat (edited by). A world without privacy. What law can and should do? Cambridge University Press.
11. Buttarelli G. (1997) B*anche dati e tutela della riservatezza: la privacy nella società dell'informazione* [Data bases and protection of privacy: privacy in the information society]. Milano, Giuffrè.
12. Cavoukian A., (2015) *Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism* // S. Gutwirth, R. Leenes, P. de Hert (edited by). Reforming European Data Protection Law // Law, Governance and Technology Series. vol. 20. Springer.
13. Clarke R., (2015) *Data retention as mass surveillance: the need for an evaluative framework* // International Data Privacy Law. Vol. 5. No. 2.
14. Colonna L., (2014) *Article 4 of the EU Data Protection Directive and the irrelevance of the EU – US Safe Harbour Program?* // International Data Privacy Law. Vol. 4. No. 3.
15. Cortese B., (2013) L*a protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona* [The protection of personal data in EU law after the Lisbon Treaty] // Diritto dell'Unione Europea [European Union Law]. 2/2013.
16. De Hert P, (2014) *The EU data protection reform and the (forgotten) use of criminal sanctions* // International Data Privacy Law. Vol. 4. No. 4.
17. Forgò N., (2015) *My health data – your research: some preliminary thoughts on different values in the General Data Protection Regulation* // International Data Privacy Law. Vol. 5. No. 1.
18. Fritsch C.,(2015) *Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite* // S. Gutwirth, R. Leenes, P. de - Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
19. Gonzalez Fuster G.,(2014) *The emergence of personal data protection as a fundamental right of the EU* // Law, Governance and Technology Series. Vol. 16. Springer.
20. Geminn C.L., Roßnagel A., (2015) *A Systematic Approach to the Legal Evaluation of Security Measures in Public Transportation* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer 2015.
21. Grau R.R., (2015) *Models and Tools for the Computational Support of Technology Impact Assessments, Applied in the Context of Mass Transportation* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
22. Gutwirth S.,Leenes R., de Hert P. (edited by),(2015) *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
23. Hempel L.,Lammerant H., (2015) *Impact Assessments as Negotiated Knowledge* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
24. Jòri A., (2015) *Shaping vs applying data protection law: two core functions of data protection authorities* // International Data Privacy Law. 2015. Vol. 5. No. 2.

25. Kiss A., Szòke G.L., (2015) *Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
26. Klitou D., (2014) *Privacy-Invading Tecnologies and Privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century* // Information Technology and Law Series. Vol. 25. Asser press – Springer.
27. Korenhof P., Ausloos J., Szekely I., Ambrose M., Sartor G., Leenes R, (2015) *Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series, vol. 20, Springer.
28. Kulesza J., (2014) *Transboundary data protection and international business compliance* // International Data Privacy Law. Vol. 4. No. 4.
29. Kuner C., Cate F.H., Millard C.,Svantesson D.J.B., Lynskey O.,(2014) *When two world collide: the interface between competition law and data protection* // International Data Privacy Law. Vol. 4. No. 3.
30. Leese M., (2015) P*rivacy and Security – On the Evolution of a European Conflict* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
31. Richards N.M., (2015) *Four Privacy Myths,* in A. Sarat (edited by), *A world without privacy. What law can and should do?* Cambridge University Press.
32. Sarat A.(edited by),(2015) *A world without privacy. What law can and should do?* Cambridge University Press.
33. Sparrow E., Halpin H., (2015) L*EAP: The LEAP Encryption Access Project,* in S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
34. Stevovic J., Bassi E., Giori A., Casati F., Armellin G., (2015) *Enabling Privacy by Design in Medical Records Sharing* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
35. Trepte S., Teutsch D., Masur P.K., Eicher C., Fischer M., Hennhöfer A., Lind F., (2015) *Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale"* (OPLIS) // S. Gutwirth, R. Leenes, P. de Hert (edited by) *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
36. Valkenburg G., (2015) *Privacy Versus Security: Problems and Possibilities for the Trade-Off Model* // S. Gutwirth, R. Leenes, P. de Hert (edited by), *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.
37. Van der Sloot B.,(2014) *Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation* // International Data Privacy Law. Vol. 4. No. 4.
38. Weber R.H.,(2014) *Privacy management practices in the proposed EU regulation* // International Data Privacy Law. Vol. 4. No. 4.
39. Zanfir G.,(2015) *Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right* // S. Gutwirth, R. Leenes, P. de Hert (edited by) *Reforming European Data Protection Law* // Law, Governance and Technology Series. Vol. 20. Springer.

**REPORTS AND STUDIES**

1. Federal Trade Commission, I*nternet of things. Privacy & Security in a Connected World,* Staff Report, January 2015 // https://www.ftc.gov.
2. EU Agency for Fundamental Rights, ECHR, Council for Europe, *Handbook on European data protection law.* 2014.

# ОТ ЗАЩИТЫ ДАННЫХ ДО «ЗАЩИТЫ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ ПУТЕМ ИССЛЕДОВАНИЯ». РАЗМЫШЛЕНИЯ В СВЕТЕ НОВОГО ЕВРОПЕЙСКОГО ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ИНФОРМАЦИИ.

В статье описывается процесс, который привел к принятию нового европейского регламента по защите данных в контексте быстрого развития информационно-коммуникационных технологий и резкого увеличение потоков данных (Большие данные). Защита данных и защита права на неприкосновенность частной жизни могут

рассматриваться в качестве ограничения для развития технологий. С другой стороны, быстрое развитие интеллектуальных городов и ИКТ приносит новые риски для защиты основных прав. Новый европейский регламент №. 2016/679 может быть недостаточным для защиты права на неприкосновенность частной жизни в эпоху больших объемов данных. Возможно, необходим какой-то новый инструмент для защиты персональных данных и, следовательно, неприкосновенности частной жизни. В статье предлагается понятие «неприкосновенность частной жизни путем исследования» как новый метод проектирования для устройств, баз данных и приложений обеспечивающий неприкосновенность частной жизни.

Хотя авторство идеи совместное, разделы 1, 2, 3 написаны С. Калцолайо, а разделы 4 и 5 написаны В. Паньянелли.

Симоне Калцолайо,
исследователь конституционного права,
Университет г. Мачерата, Италия.
Валентина Паньянелли,
адвокат, г. Мачерата, Италия.

**Ключевые слова:**
информационные и коммуникационные технологии, Большие данные, европейские персональные данные, защита права на частную жизнь в ходе конструирования, защита права на частную жизнь путем исследования, Habeas Data.

**Keywords:**
Information and Communication Technologies – Big data – European Personal Data – Privacy by Design – Privacy by Research – Habeas Data.