The centrality of the individual in the digital society

Fabrizia Rosa
Università degli Studi di Napoli Parthenope, Naples (IT)

ABSTRACT

The social and economic reality in which we live in this historical moment is strongly influenced by the development of digital technologies and this requires, unlike in the past, the need to put the person and his rights at the center of development.
This contribution aims to analyze the changed relationship between privacy (protection of personal data) - in its social and collective dimensions - and security (which, as a collective interest in the overall holding of the rule of law, has been greatly strenghtened).
If you pass the simplified dichotomy "privacy vs security" and look deeper into the needs on which the two rights and constitutionally protected goods are based, it can be concluded that, in certain cases, national security and public security needs may involve specific limitations on the right to privacy and data protection, but never involving the complete sacrifice of one or the other protected legal position.
The most important focus of this discussion is a reflection on the fundamental choices to which our civilizations are called and the challenge that the western world must take with respect to a technological evolution.

Keywords
individual; society; privacy; security; technological development

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction the individual as the centre of technological development

In a socioeconomic context so strongly influenced by the development of digital technology and its constant evolution, a change from past perspectives is absolutely necessary, to the end of placing the individual and her rights at the centre of development.
The Universal Declaration of Human Rights of 1948, although not elevated to being the source of general international norms, opened the way to the drafting of various documents and charters dedicated to human rights, the most important of which is surely the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed by the member states of the Council of Europe on November 4th, 1950.
The last step towards a project of codification of fundamental rights is represented by the Charter of Fundamental Rights of the European Union, officially proclaimed in Nice on 7 December 2000 and known as the Charter of Nice.
The importance of these documents (and, with them, also those that followed) lies, above all, in having provided evidence of the recent change in the relevance of the person in the international context.
In fact, until the end of the 19th century, the subjects of the international community were States and Governments, while man was only relevant as a member of a given community, as part of a whole, and only as such he was considered worthy of protection and entitled to rights. From this conception, it derived that the person, having no specific weight, was detectable outside his or her national borders only as a foreigner.
Recently, however, the evolution and change of society has meant that man has finally seen a role and a weight never obtained before: man is a subject in himself considered, regardless of his nationality, worthy of consideration, protection and protection as such and not because he belongs to a group.
Therefore, the protagonists of the international framework are no longer only sovereign states, but also the individual, who from being a member of higher entities rises to the rank of individual. Her rights and freedoms are highlighted as inviolable rights that she is entitled to simply because she exists, which any center of power must "recognize" as pre-existing and with which it must not interfere.
This change of conception is clearly linked to the incessant change of society, and not to codification. Within this framework, the international charters have established universal rules valid for all nations and for the protection of every individual, but the attention to fundamental human rights is not due to these, but rather to the imposition of the individual, his dignity and his needs on the international sphere. This, together with the rapid development of technological and medical sciences, has led to the emergence (and

continuous emergence) of new rights, in the past neither configured nor configurable, imposed on governments as fundamental because they are rooted in human dignity and culture.

In particular, the development of digital technologies (and, last but not least, the advent of artificial intelligence), strongly influencing the social and economic reality in which we are living in this historical moment, has required a radical change of perspective compared to the past, in order to put the individual and his rights at the center of development. In fact, it is believed that the development of digital society puts individual freedom and the fundamental rights of individuals at risk, because where it is true that technology favors the collection of new and different types of information useful to document human rights violations (for example in insecure and inaccessible areas, Amnesty International has used satellite images to document the massive destruction of civilian infrastructure in Syria), it is also true that new information and communication technologies are producing more and more capillary and invasive forms of control in the private sphere of each one of us, bringing into question consolidated fundamental rights and freedoms (just think of the spread of video surveillance, the filing of fingerprints, the extension of control to Internet traffic).

It is evident that, due to the very way in which it (the digital society) is "constructed", the individual inevitably becomes part of a collective mechanism: the relationship between individual and social group is no longer a relationship of freedom, but a mechanistic relationship of belonging, whereby everyone becomes at the same time producer and consumer, employee and employer and supplier of the information necessary for the overall system to take care of him and so that he may benefit of an all-embracing social ordering that, however, ensures his well-being and attention (**D'ACQUISTO, 2017**).

Well, with such centrality of the individual, priority issues emerge such as rights and freedoms.

In particular, here we want to focus on the changed relationship between privacy (today generally understood as protection of personal data, but in reality the two concepts can also be kept separate) - as a fundamental right whose purpose is the maintenance of a space of freedom for the individual and his or her centrality, especially in a social and economic context so strongly influenced, as seen, by the development of digital technologies - and security.

Therefore, the contrast between freedom technology and control technology is becoming stronger and stronger.

The right to privacy: social dimension and collective dimension

The term "privacy" now refers to the right to confidentiality of personal information and private life. But let's take a step back.

Initially, this right was considered in the different areas of protection of physical freedom, home, secrecy of correspondence, freedom of association and freedom of expression.

Only later did it begin to assume its own conceptual autonomy, its own legal consistency and its own recognition, even of constitutional rank. In particular, this step took place thanks to the essay "The Right to Privacy" (**WARREN & BRANDEIS, 1890**) by S. Warren and L.D. Brandeis of 1890, in which the term "right to be let alone" is used, (modern formula of "jus solitudinis"): it was configured as a right of the person to exclude any foreign interference within the home, to enjoy one's life in peace.

However, the thesis put forward by the two American jurists was not immediately accepted by U.S. jurisprudence and several decades passed before the affirmation of the right to privacy as a constitutional right in the U.S. constitutional order.

Turning to the European framework, the road to the constitutional affirmation of the right to privacy is different.

Until the end of the 1980s, individual countries moved in a scattered order. On the one hand, there are countries in which national Constitutions dedicate ad hoc norms to the protection of privacy or confidentiality in the proper sense, which are therefore easily recognised. But there are also other countries, such as Italy, where the Constitution does not contain a single rule dedicated to confidentiality.

In our system, in fact, the constitutional recognition of the right to privacy was based, on the one hand, on the assumption that Article 2 of the Constitution, placing the individual at the center of the system, allowing the recognition of

rights even outside those set forth in the Constitution itself; on the other hand, on a joint reading of Articles 13, 14, 15 and 21 of the Constitution, which each protect and guarantee different profiles of privacy of individuals.

Soon, however, the concept of confidentiality as the "right to be left alone" widens and begins to be understood also as a claim of control over one's own personal data.

In fact, since the 1980s, first thanks to the ECHR and the Strasbourg Court, and then thanks to the European Union, European data protection law came into play.

Initially, this right protected only the profile of the right to privacy connected with the processing of personal data and the control of one's own data, while the recognition of the aspect of exclusive knowledge of one's own affairs, which was the dominant profile, was left to the individual States.

However, technological development is gradually eroding this original distinction, in the sense that, while it is true that there is still some room for national legislators, especially in the balance between confidentiality and freedom of expression and between confidentiality and transparency, it is also (and above all) true that, thanks to the ability of European legislation to offer ever stronger solutions and protections, the initial relationship has been turned upside down, so that today it can be said that the European model of protection of confidentiality coincides with data protection, on the understanding that European legislation leaves some areas to the State, albeit always within the overall model.

In particular, with the development of technologies and with the increasing use of the processing of personal data, and the possibility of their exchange and aggregation across the Internet and the creation of databases, the requirements related to privacy have evolved and continue to evolve. In fact, the continuous collection of information means that almost all actions and individual choices made by man leave traces, to the extent that the expression "electronic body" has been coined.

One of the risks connected to this evolution is the possibility of creating a society of surveillance and classification, "in which relentless control over people erases rights and causes democracy to deteriorate" (**RODOTÀ, 2004, A**) . A fitting example could be the transition from targeted forms of surveillance to generalized forms of surveillance, such as those introduced in the United States, after the attacks of September 11, 2001, with the Patriot Act, through which the U.S. authorities demanded data regarding the use of credit cards by travelers from Europe.

Or, to be even more topical, the use - at the time of the COVID-19 - of applications and systems for tracking people so that positive results can be located along with those who came into contact with them.

In this way, interest in privacy has become an interest no longer of the individual, but of the entire collective, with the consequence that the expression "protection of privacy" no longer refers only to traditional aspects (which can be traced back to the so-called right to be left in peace and its evolution), but also to the power to control the circulation of one's personal information

As proof of this, one should bear in mind that in international language the most widely used expression is now that of data protection.

At the European level, the Charter of Fundamental Rights of the European Union distinguishes, not without reason, the respect for private life and the protection of personal data, provided respectively by art. 7 and art. 8. The reason for this distinction lies in the fact that the right to respect for private and family life has a mainly individualistic nature and the respective power is essentially limited to excluding interference by others: in this case, the protection is static and negative. Data protection is different as it sets rules on how data is processed and takes the form of powers of intervention: here the protection is dynamic and follows the data in its circulation (**RODOTÀ, 2004, B**) Precisely this distinction marks the path and evolution of the concept of "privacy", from the right to be left alone to the right to maintain control of one's own information and to determine how one's privacy is constructed. This has signified , especially in recent years and indirectly, the strengthening of the awareness of a real "right to self-determination", as the right to build one's own personality, with the consequent need to freely make choices consistent with one’s principles (this especially in health care).

Moreover, again at the European level, the powers of control and intervention are attributed not only to the individuals concerned but also to an independent Authority, thus further highlighting the move "from the consideration of privacy as a

pure expression of an individual need to its placement within the framework of the new 'electronic citizenship'. We are, thus, facing an aspect of individual and collective liberality, an interminable guarantee against any form of power, whether public or private"

In fact, the mass development of technologies, the particular invasiveness of some of them and the growing possibility of their mutual interaction, with the consequent exchange of information and collected data, exponentially multiply the risks of violation of the right to privacy.

This is why EU Regulation 2016/679 intervenes, which aims to ensure and strengthen the free circulation of data, preventing, however,that this and the development of the digital society can take place to the detriment of fundamental rights and individual freedoms of citizens. and those residing in the EU.

And this is why, within this Regulation, two other fundamental guarantees are introduced, in addition to confidentiality, to protect the security of data processing: the availability and integrity of the data of the person concerned.

The protection of personal data, understood with the two additional guarantees, represents, therefore, an evolution of privacy understood as the right to confidentiality. So much so that the European legislator has taken care to provide clear indications to the data controller and data processor in order to adopt "adequate technical and organizational measures to ensure a level of security appropriate to the risk". The reasons for this are to be found in the technological and IT evolution recorded in public and private organizations and in the increasingly pervasive use of social networks that have led to an increase in the risks that users now take on a daily basis through the communication and dissemination of personal data.

This risk, connected to a still more accelerated profiling deriving from the systematic adoption of ever more sophisticated algorithms that can even be predictive of our behaviour, not only in purchases or sales but also in our work performance.

From what has been said so far, it is clear that with the advent of digital society, it was necessary to think about the security of personal data as the Internet can, yes, be the prerequisite for expansion, but can also be a source of limitation of freedoms.

Security

The security of individuals has been an individual right from the beginning. Just think of the Hobbes doctrine of the State, based on the search for survival and the intrinsic value of security: individuals transfer their natural rights to a subject (who, in Hobbes' reconstruction, is the sovereign) who has the necessary strength to oppose anyone who wants to break the peace of the State.

Still, in contemporary constitutional systems the qualification of security as an individual right has become residual. In fact, today it is believed that individual security consists in the contextual and overall protection of constitutional assets or the security of rights. From this follows the breaking of the link between security and coercion, projecting itself towards a guarantee of individual security through actions in support of the effective enjoyment of constitutionally protected rights (**DOGLIANI, 2010**).

But if on the one hand, in contemporary constitutionalism, we see the weakening of the right to security as an individual right, on the other hand, the principle of security as a collective interest in the overall maintenance of the rule of law has been greatly strengthened, with the consequence that, in the current Constitutions, the constitutional value of state security, national security, public safety and public order is recognized

Let us now analyze the relationship between security (in both its meanings, individual and collective) and the right to privacy.

Starting from the concept of security as a collective interest, it should be borne in mind that both national security and public safety are considered, both by the ECHR and the Charter of Fundamental Rights of the European Union and the Italian Constitution, as legitimate purposes to impose, under certain conditions, limitations on the right to the protection of personal data.

In this regard, all the regulatory acts of the historic European corpus of data protection (Directive 95/46, the so called mother directive, later repealed by Regulation 679/2017 and Directive 680/2017, Directive 58/2002, the so called e-privacy directive and Decision 2008/977/JHA on the processing of data for judicial cooperation in criminal matters and police operations) specify that the European rules leave unchanged the existing balance between citizens' right to privacy

and the possibility for Member States to take the necessary measures to protect public security, defence, state security and criminal law enforcement. However, Directive 58/2002 takes up the case law of the Court of Justice and states that any limitations to the right to data protection must comply with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the judgments of the Strasbourg Court.

The new European legal framework, and in particular the new Regulation 679/2017, provides - as will be seen in more detail in the following paragraph - important specifications regarding the content of any restrictions and taxable limits. First of all, it is clarified that the restriction must be necessary and proportionate in a democratic society, which recalls the formula contained in both the ECHR and the Charter of Fundamental Rights of the European Union. In addition, it is provided that the restriction, when legislation is adopted, must contain some specific provisions about, for example: (i) the purposes of processing or the categories of processing; (ii) the categories of personal data; (iii) the scope of the restrictions introduced; (iv) the guarantees to prevent abuse or unlawful access or transfer; (v) the right of data subjects to be informed of the restriction, unless this would compromise the purpose of the restriction; (vi) the precise indication of the data controller or the categories of processing.

From this it can be seen that the "test of legitimacy" of any future and possible restrictions is expected to be very severe, but in line with the most recent case law of the ECHR and the Court of Justice. As regards the former (the case law of the ECHR), the case law on the protection of privacy and personal data protection is very substantial (and sectorial).

The case law of the Court of Justice, on the other hand, consists, above all, of the judgments Digital Rights Ireland and Schrems, two cases which are very well known and on which there is now a broad doctrine

In any case, all the judgments of the Courts (both in Strasbourg and Luxembourg) deny the simplification "privacy vs. security", stating that neither must be sacrificed and, in particular, that the essential core of the individual right to the protection of personal data must be preserved.

Moving on to discuss the relationship between protection of individual security and protection of personal data, it can be immediately noted that there are significant similarities, both if the declination is that of the right to security as security of rights, and if reference is made to the right to security as an individual and autonomous right.

In favour of the first conception (security as security of rights), there is the consensus, as also confirmed by the European Regulation that the right to data protection is now both the inalienable protection of all freedoms and a general interest of society. In fact, the new regulatory apparatus is aimed at strengthening the degree of protection through a series of innovations such as the empowerment of data controllers and data processors; the mandatory provision, in some cases, of a Data Protection Officer; the obligation to adopt mechanisms of privacy by design and by default and so on.

If, instead, one prefers to define the right to security as an individual and autonomous right, then the protection of personal data, including its institutions, obligations, controls, guarantees and sanctions, represents an important barrier against the risks that emerge in our digital society, (risks) related to criminal behavior against individuals (e.g. identity theft).

These considerations are supported by the rules of the above mentioned Regulation, which define the security principle as the cornerstone of data processing and require data controllers to assess ex ante, depending on the data processed and the purposes of processing, the risks and to adopt, consequently, all technical and organizational measures necessary to minimize them, especially where they may affect the rights and freedoms of individuals

An example of limitation of the right to privacy (as an individual freedom) in favor of security (as a collective interest): the processing of personal data at the time of COVID-19.

The right to privacy - as previously mentioned - like other fundamental rights, is not absolute and, therefore, may be restricted for the pursuit of an objective of overriding general public interest or to protect the rights and freedoms of others. In fact, it falls within the scope of Article 52(1) and (3) of the EU Charter, which provides that a specific primacy can be given - if certain conditions are met, including without doubt

emergency situations in the health sector - to the objectives of general interest, enshrined in Article 3 of the Treaty on European Union (TEU).

In recent months, in particular, the health emergency caused by COVID-19 has made it necessary to balance collective interests (in particular, the protection of public health - contained in Article 35 of the Charter of Fundamental Rights of the European Union) and individual freedoms (including: respect for private and family life (Article 7 Charter) and the protection of personal data (Article 8 Charter)).

In this context, in fact, the collection and use of data, and in particular those relating to health, have been and still are indispensable tools in the action to combat and contain the pandemic.

However, in such a framework, one should not underestimate the risks that may arise for the rights and freedoms of individuals. To this end, it is useful and, even more so, necessary to draw a line between initiatives that prove to be effective as measures to contain the spread of the virus and those that, instead, fall outside this objective and are aimed at accumulating data for purposes of trade promotion or surveillance (**BRIGANTE, 2020**).

The ongoing health emergency, therefore, requires careful reflection on the evolution of the relationship between privacy and public health and the importance of the public interest in the processing of personal data.

The problematic point concerns the identification of the permitted level of limitation of rights, that which is strictly necessary for health protection purposes. In other words, it seems more than legitimate to ask: how far can the tension created between privacy and public health go?

In order to answer this question and in order to understand the extent of the balance between collective interests and fundamental freedoms, it is necessary to examine the rules that are relevant in this case in terms of privacy.

In particular, it is necessary to examine the provisions of EU Regulation 679/2016 (hereinafter GDPR), in Article 23, paragraph 1; in recital no. 4; in article 6.1, letter e); in Article 9, paragraphs 1 and 2.

Article 23(1) and Recital 4 of the GDPR introduce some possible limitations to the application of the principles on the protection of personal data, when necessary to protect general interests assessed as prevailing, in compliance with the principles of proportionality, necessity, security and when aimed at the pursuit of objectives of general interest recognized by the EU or linked to the need to protect the rights and freedoms of others (in accordance with Article 8 ECHR and Article 52, EU Charter).

According to Article 6.1(e), GDPR, processing is lawful when "necessary for the performance of a task carried out in the public interest or connected with the exercise of official authority vested in the controller".

Finally, Article 9, paragraph 1, GDPR states that "It is forbidden to process [...] data relating to health", providing in paragraph 2 a long list of hypotheses of inapplicability of the general provision referred to in paragraph 1 and, therefore, of exceptions that make such processing lawful, including: processing necessary for reasons of public interest relevant under EU or Member State law; for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and medicines and medical devices [...]; for purposes of treatment, i.e. preventive medicine, diagnosis, health or social care or therapy or management of health or social systems and services [...].

According to the European Legislator, therefore, "The right to the protection of personal data is not an absolute prerogative, but must be considered in the light of its social function [...]". (Considering 4 GDPR).

Well, in the current state of emergency - given the close connection between personal privacy and public safety (and, why not, the digital world) and the need to give precedence to collective security (and health) over the protection of individuals' personal data - the attention of all States has been turned to the extraordinary nature of the measures adopted and to be adopted.

Even still, since not all Member States have adopted the same (more or less restrictive) conduct, a need has emerged to outline a common line of action between the different countries of the European Union, hoping for a pronouncement of the EDPB (European Data Protection Board or the European commission on the protection of data) on this point, in order to further harmonize the discipline at supranational level and to avoid dangerous uncertainties of interpretation.

The Committee expressed its opinion on this issue on March 19, 2020, publishing a "Statement on

the processing of personal data in the context of the COVID-19 epidemic", which, although it has not clarified all the issues discussed, offers some interesting food for thought.

In particular, the EDPB stressed that the current pandemic is a legal condition that can legitimize restrictions of freedoms, provided that they are proportionate and limited to the emergency period. With regard to the lawfulness of processing, the GDPR allows public health authorities and employers to process personal data during an epidemic.

As far as of interest, the GDPR provides for exemptions from the prohibition of processing of certain special categories of personal data, such as health data, if this is necessary for reasons of public interest relevant to public health (Article 9.2(i)) on the basis of Union or national law, or where there is a need to protect the vital interests of the data subject (Article 9.2(c)), since recital 46 makes explicit reference to the control of an epidemic.

The Declaration also addresses the issue of the processing of location data for smartphones, stating that public authorities should, first and foremost, seek to process location data anonymously and in an aggregate form. As known, in fact, preference should always be given to the least intrusive solutions, taking into account the specific objective to be achieved. On the contrary, more intrusive measures may be considered proportionate in exceptional circumstances and depending on the concrete modalities of processing. In such cases, the measures taken should in any case be subject to reinforced control and more stringent guarantees.

In any case - as anticipated - the indications provided by the Committee remain generic and do not offer a definitive solution to the issues addressed, but other clarifications will probably also come from the different national privacy authorities, considering that Member States seem to follow different approaches, especially with regard to the technological monitoring of the spread of the virus.

Conclusion

Over the last decades, the advent of a "digital society" has meant that man has played an increasingly central role within it, leading to the emergence of new needs and, therefore, new rights.

This has been followed by a transformation, or rather an extension, of one of the fundamental rights of the individual, namely the right to privacy, which "from being a protective shell of the person is evolving to a circulating information heritage, as a common denominator of all industrial, commercial, cultural, public and private realities and as a constant reference for all fields of activity" (**SANTANIELLO, 2004**).

In fact, today we refer not only to the person - both as an individual and in the social formations with which he or she relates - but also to democratic processes, which are influenced by the way information circulates. Consequently, the instruments of protection must be adapted to the evolution of technological innovations. And indeed, the Commission first and the European legislator afterwards, in accordance with the principles of subsidiarity and proportionality and in order to "create a global, coherent, solid and modern framework for data protection in the European Union", have decided to reform the area in question through the instrument of the Regulation, which presents significant innovations compared to the previous legislation (**BRUGIOTTI, 2013**).

In particular, Regulation 2016/679 focuses on the security of data processing, risk minimization, on the obligations incumbent on the data controller and on sanctions. In this regard, it is emphasized that collective security requirements are not satisfied with the generic compression of citizens' privacy, but, on the contrary, with its strengthening: privacy (or data protection) and security are complementary and not alternatives, since data protection is not only an individual right but a primary interest of the community and society. Therefore, it is instrumental, on the one hand, to the guarantee of rights and, on the other, to the overall stability of democratic systems (**OROFINO, 2018**).

From this it emerges that, since data protection is necessary both to guarantee security as security of rights and security in the subjective sense as the ultimate glue of societies, the dichotomous expression "privacy (data protection) vs. security" is not suitable to describe reality, and should instead be changed into the opposite statement "privacy (data protection) is security".

However, in some cases, national security and public security requirements may result in specific limitations of the right to privacy and data protection. This, however - as also the jurisprudence of the European Courts has stated - can never (and must never) entail the complete sacrifice of one or the other protected legal position. In fact, both Courts, in relation to the balance between data protection and security needs, have contributed to define the impassable stakes and the minimum or essential content of the right to data protection, recalling the principle of strict necessity of the limitations actually adopted.

Precisely in analyzing such a balance and in order to identify appropriate tools to ensure a fair balance between the two rights (privacy and security), this discussion wants to invite a reflection on the fundamental choices to which our civilizations are called and the challenge that the world must face of the risks that would involve an evolution of "out of control" digital technology .

Indeed, the spectre of data breach should never be underestimated, because data breaches - especially in difficult times such as the current one caused by the COVID-19 emergency - are just around the corner. In fact, the importance of personal data protection regulations and IT security investment plans, aimed at channelling the flow of Big Data in the healthcare sector, has emerged more and more recently; issues that make it necessary to put in place adequate strategies for the protection of databases and sites of public and private entities, with particular regard to hospitals.

Therefore, if we want to defend our rights and freedoms (of individuals but also of the community) it seems more important than ever to employ resources on the cybersecurity and national cybernetic security front, because the ever increasing store of information and digital heritage can jeopardize the protection and confidentiality of data processed.

From what has been said so far, it is clear that the use of Big Data can be an opportunity, provided, however, that the expectations of those concerned are met and their privacy is guaranteed.

Here we can conclude that the path of the right to privacy is far from over.

References

[1] Barbera A. (2001), La Carta europea dei diritti: una fonte di ricognizione?, Diritto Unione Europea, 2-3, p. 241.

[2] Bifulco R. (2016), La sentenza Schrems e la costruzione del diritto europeo della privacy, Giurisprudenza costituzionale, 1, p 289 ff.

[3] Brigante F. (Aprile 2020), Imprese e diritti umani. Le interferenze con il diritto alla privacy durante l'emergenza COVID-19: un delicato bilanciamento tra diritti. [Online] Available: www.peridirittiumani.com.

[4] Brugiotti E. (Maggio 2013), La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico. [Online]. 2. Available: www.dirittifondamentali.it

[5] Chiti, M. P. (2002), La Carta Europea dei diritti fondamentali: una carta di carattere fondamentale?, Rivista Trimestrale Diritto Pubblico, 1, 1.

[6] Curicciati L (2017), Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della Data Retention Directive, Democrazia e sicurezza, 2.

[7] D'Acquisto G. & Naldi M. (2016), Big data e privacy by design, Giappichelli, Torino, pp. 41 ff. and 117 ff.

[8] De Minico G. (2016), Antiche libertà e nuove libertà digitali, Giappichelli, Torino, p. 136.

[9] De Siervo U. (2000), L'ambiguità della Carta dei diritti fondamentali nel processo di costituzionalizzazione dell'Unione Europea, Diritto Pubblico, pp. 50 et seq.

[10] Dogliani M. (2012), Il volto costituzionale della sicurezza, in G. Cocco (ed.), I diversi volti della sicurezza, Giuffè Francis Lefebvre, Milano, 1 ff.; (2010), Astrid Rassegna, 22, p. 6.

[11] Falletta P. (Dicembre 2015), La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C – 362/14). [Online]. 24. Available: www.federalismi.it

[12] Giupponi T.F. (2008), La sicurezza e le sue "dimensioni" costituzionali in AA.VV., Diritti umani: trasformazioni e reazioni, Bononia University Press, Bologna, 275 ff.

[13] Martines T. (2005), Diritto costituzionale XI ed. entirely revised by G. Silvestri, Giuffè Francis Lefebvre, Milan., pp. 584.

[14] Niger S. (2006), Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali, Cedam, Padova.

[15] Orofino M. (Giugno 2018), Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione. [Online]. 2. Available: www.medialaws.eu,

[16] Pace A. (2001), A che serve la Carta dei diritti fondamentali dell'Unione Europea?, Giurisprudenza Costituzionale, pp. 193 et seq., 207.

[17] Pavani G., Concetto e ambito dei nuovi diritti. [Online] Available: www.filodiritto.com

[18] Petti G.B. (2006) , La Costituzione europea e la tutela civile dei diritti umani, Maggioli Editore, Rimini.

[19] Pollicino O. & Bassini M. (2016), La Carte dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo, in G. Resta & V. Zeno Zencovich (ed.), La protezione transnazionale dei dati personali. Dal "Safe Harbour principles" al "Privacy Shield", Roma Tre-Press, p. 73 ff.;

[20] Pollicino O. (2015), La "transizione" dagli atomi ai bit nel reasoning delle Corti europee, Ragion pratica, 44, p. 53 ff.

[21] Pollicino O. (Novembre 2014), Interpretazione o manipolazione? La Corte di Giustizia definisce un nuovo diritto alla privacy digitale. [Online]. 3. Available: www.federalismi.it - focus TMT.

[22] S. Rodotà (Ottobre 2004, A), Apologia dei diritti. [Online]. Available: http://it.scribd.com/doc/53206551/Apologia-dei-diritti-Stefano-Rodota-I-diritti-dell-uomo-oggi-Norberto-Bobbio.

[23] S. Rodotà (2004, B), Tra diritti fondamentali ed elasticità della normativa, Europa e diritto privato, 1, p. 1-12.

[24] Rodotà S. (Ottobre 2004), I nuovi diritti che hanno cambiato il mondo. [Online]. Available: www.privacy.it.

[25] Rodotà S. (2002), Introduzione a David Lyon La società sorvegliata. Tecnologie di controllo della vita quotidiana, Feltrinelli, Milano.

[26] Rodotà S. (1995), Tecnologia e diritti, Il Mulino, Bologna.

[27] Ruggeri A. (2001), La forza della Carta Europea dei diritti, Rivista Diritto Pubblico Comparato Europeo, p. 184.

[28] Ruotolo M (2013), Diritto alla sicurezza e sicurezza dei diritti, Democrazia e Sicurezza, 2, 4 ff

[29] Santaniello G. (Giugno 2004), Tipologia delle innovazioni tecnologiche e protezione dei dati personali, in Innovazione tecnologica e privacy. [Online]. Available: www.garanteprivacy.it.

[30] Tiberi G. (2007), Riservatezza e protezione dei dati personali, in M. Cartabia (ed.), I diritti in azione, Universalità e pluralismo dei diritti fondamentali nelle Corti europee, Il Mulino, Bologna, p. 351.

[31] Warren S. & Brandeis L.D (1980), The right to privacy, in Harv. L. Rev., 1890, 4, 193 e ff