Mestrado em Segurança da Informação e Direito no Ciberespaço

The Walking Virtually Dead: Entre uma Algoritmocracia Jus Constituendum e um Homem Virtual Transparente, Existe Espaço para o Direito a uma Identidade Informacional?

NUNO TEIXEIRA CASTRO

DISSERTAÇÃO PARA A OBTENÇÃO DO GRAU DE MESTRE

em

SEGURANÇA DA INFORMAÇÃO E DIREITO DO CIBERESPAÇO

ORIENTADORES:

Professor Doutor EDUARDO VERA-CRUZ PINTO
Professor Doutor CARLOS CALEIRO

JÚRI:

PRESIDENTE: Professor Doutor PAULO MATEUS (IST)

VOGAL: Professor Doutor EDUARDO VERA-CRUZ PINTO (FDL)

VOGAL (ARGUENTE): Professor Doutor ALEXANDRE SOUSA PINHEIRO (FDL)

OUTUBRO DE 2016

Porque sem eles a nossa essência nunca seria a mesma,

À minha família,

Em particular à Raquel e ao meu Princípe.

NUNO TEIXEIRA CASTRO

ÍNDICE

LISTA DE ABREVIATURAS

AC.- Acórdão

ACT.- Autoridade para as Condições do Trabalho

AT. – Autoridade Tributária e Aduaneira

C.A.D.A. – Comissão de Acesso aos Documentos Administrativos

CGA- Caixa Geral de Aposentações, I.P.

CNPD – Comissão Nacional de Protecção de Dados

CRP – Constituição da República Portuguesa de 1976

DPD - Directiva 95/46/CE

EM – Estados-Membros

L.A.D.A. (2007) – Lei n.º 46/2007, de 24 de Agosto – LEI DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS.

L.A.D.A. (2016) – Lei n.º 26/2016, de 22 de Agosto - LEI DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS, aprovou o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Directiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de Janeiro, e a Directiva2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de Novembro.

LDPD - Lei n.º 67/98, de 26 de Outubro - LEI DA PROTECÇÃO DE DADOS PESSOAIS (transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados).

RGPD - Regulamento (UE) 2016/679 Do Parlamento Europeu E Do Conselho de 27 de abril de 2016, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (*Regulamento Geral sobre a Proteção de Dados*).

RTBF - *Right to Be Forgotten*

SS.- Segurança Social

TC – Tribunal Constitucional

TJUE – Tribunal de Justiça da União Europeia

"The Web is like an elephant — it never forgets, and if let loose it can cause a lot of trouble"[1]

1 SULLIVAN, Paul, *Negative Online Data Can Be Challenged, at a Price*. (10/06/2011) NYTimes, disponível em: http://www.nytimes.com/2011/06/11/your-money/11wealth.html - Último acesso Set.2016.

EXTENDED ABSTRACT:

First of all, we want to highlight our bibliographical options made. We do believe in two major, yet simple, things: knowledge should and must be faced as one basic human and fundamental right; access to it (to knowledge) should be free, open source, available, accessible, *searchable*. The internet can make this possible. We dare to say that only if we take this commitment as deeply valid as we must, only then the society will evolve as a whole and as it should, taking *that* advantage of the immense potential that internet, as *the tool*, provides us. Nevertheless, we must underline that we are not in favor of a "*non-recognition of the credits*" held and materialized by others and their means. Let's state it very clearly about *copyright issues*: in order to prevent plagiarism, one must give appropriate credit to its author, either by providing a link to his authorial work, either by using his work in a reasonable manner[2]. The credit should be where it belong in the first place. Naturally. You may well take us as a "*dreamer*", but, insofar one can maintain and pursue mutual respect, all the society will have so much to receive.

Once already clarified this first kicking-premise, we must now focus on the main subject of our dissertation: is there a way to erect a right to informational identity?

Today, in the age of global information society, the unstoppable evolution of electronic communications systems, of global communication network, of *Internet all the time and all over the place*, the collection, capture, annexation, indexing and mass transmission of Big Data, full of personal information, identifiable or susceptible to identify an individual - one person, must undertake to revamp the entire discussion of personal data and their protection. All over the world, mostly, the focus of the discussion has been only on *datum* and its protection: either about packages, strings, files and databases, disregarding the fundamental of all this, *i.e.*, the person.

Without embarrassment, the imminent and *tempting seduction*, either by self-indulgence, ease, immediacy, accessibility and availability, of all that informational research and its results – the argumentative menu related to this temptation is always quite profitable –

2 For instance, just as Creative Commons, at: https://creativecommons.org/licenses/by/3.0/legalcode . – last access October 2016.

where the person is dismissed of most of her human dignity, transforming her into a mere informational object, urges to refocus the entire debate on the person's protection, surpassing the discussion over its fragments, like data and their protection. The present time presents us with a considerable stage of erasure of the primacy of the democratic rule of law, which is difficult to sustain and difficult to counteract. The compression of the fundamental rights of the human person tends to override their defense, in the name of a (putative) greater *sense of security*. Here lies the intense fight of jurisprudents in safeguarding the entire democratic state of rule of law.

The data protection doctrine, of German inspiration[3], recognizes the *original-failure* of its dogmatic: "*data protection*" or even "*protection of personal data*" is short as to the scope of protection that is intended. What is really at issue are not "*datum*" or their "protection", but the person, only and by herself, in all its essence of human dignity that characterizes her. Once marked this "*original-failure*", one must overcome it, starting from this human dignity, centering it around her "personal information", it is time to positivize one adequate right to informational identity.

We assume the will to search for a path that, ultimately, can lead us to stimulate the positivization of this right. For instance, facing this emergent and scathing reality of *big data*, the giant wave of information, all these informational flood that emerges and circulates and that is transmitted in the network, to what extent it restricts fundamental rights? Namely, to what extent it compresses our right to an informational identity?

Many *ordinary* (as in the real world) conflicting rights, such as the right to inform; to be informed; to access knowledge, to transmit it and to share it; freedom of opinion and expression and other related personal freedoms; safety and security; find a new stage in this *Agora* of modernity. Observing it, they lead us, therefore, to ask the following question: in that sense of the *myth* - which is crystallizing - that the Internet never forgets, do these conflicting spaces only know *one-way* movement? Indeed, think about this: One person made a mistake in her life. That mistake gained breadth with its spread over the

3 Supported in part by the decision of the German Constitutional Court of 1983, on the law of Censuses, where it was argued that the individual should participate in all stages of the processing of personal data, as well as the public authorities were also obliged to provide the necessary information to the holders of personal data when processing their data. The formula *informationelle Selbestimmung* - informational self-determination - would eventually be unraveled by this decision.

internet. If the tool (the internet) never forgets, those "*open wound*" will forever stick to that person's solely definition? Have we noticed that we are establishing one path with no room for repentance? Denying our humanity? Right to be *reborn*; right to *reformat* us; to *rebuild our identity*; *to forget and forgive;* aren't they all such typical instruments of the edification of this last, unique, unrepeatable, singular condition of each human being?

It is far from being easy, faced with such a comprehensive exposition of motives and themes, to make a singular narrowing of the reason that moves us in this current investigation. More over when we intend to discuss a Regulation *(European General Data Protection Regulation)* that will only be implemented in May 2018. Nevertheless, the simple and succinct form as we list some aspects, could allow us to delineate a given sense on it. Presupposed beforehand in the constant demand of the valuation of human dignity, the right that we want to positivize, is revealed through the combination of this ultimate principle of human dignity with the intricate rights who grant such dignity that characterizes us all.

We'll point out a varied set of resistances to its realization in the network, in the virtual world. Right away, we start with our digital footprint. Is this footprint, the one that we are leaving behind in every contact we establish either in the network and through it, so impossible to *de-index, erase, stop tracking,* to control (by its owner)? In fact, as we shall try to explain, the present imposed condition of control and management of the network by the *divine algorithm,* has overshadowed the realization, in the virtual world, of a whole array of characteristics as human as forgetting, being left alone, repenting, forgiving...a set of characteristics that makes up everyday mundane realities, so natural, so human.

Anticipating a bit, will the legal implementation of one *«right-to-be-forgotten» (Article 17 of the General data protection regulation, as one right to oblivion*) - derived from something as human as forgiving and forgetting and moving on – be so dependent on the factorization and *divine algorithmic will*? Lets put it simple: as mentioned before, is there space, in the future, for one *right to repentance* over what we concretely accomplish in our present, in the network? Will we have space to be left alone, not to be harassed, even maintaining a daily civic participation over the network? Or this aim can only be achieved if we are kept apart of the network?

The idea of being haunted by a less achieved past intrigues us. How long will it be socially acceptable for this past to haunt us? Take, for instance, the judgment handed down by the Belgian Court of Cassation, in Olivier G v Le Soir, Case n.º 15.0052f, April 29th, 2016. There, the Court decided that, as an obvious result of one *"right to be forgotten"*, the newspaper Le Soir had been properly ordered to anonymise the online version of a 1994 article concerning a fatal road traffic accident involving Olivier G. The detractors of the importance of this decision promptly counterattacked with the argument of one *dangerous* "right to rewrite the history", as if a person who had already paid either criminally or socially for a mistake he made in the past wasn't enough punishment. As if the person did not have the right to learn from this mistake in the past and rebuild herself in the present.

We do not neglect the fact that one full enjoyment of these human rights, at least in appearance, may be able to conflict with the *Code*[4] used in the coding, construction and dispersion formulas of the network, resulting in the net as we know it today. Noting a weakness in the exposure of this particular reason - mostly because technology should serve only as a complement to the natural human imperfection, and never as a means to magnify such imperfections – the presented solution is set to try to change our human nature instead of complementing and perfecting the tool? Really?

Nonetheless it is significant to notice that either due to quite strong case-law of the CJEU, either by *constant attempts*[5] to put into practice one *newest* legal framework for data protection in the European Union - which culminated in the publication in the Official Journal of the European Union of one comprehensive package of Legislative acts, highlighting Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in May 4th, 2016[6] - concepts such as privacy

4 As Lawrence Lessig posed it.

5 Take first the Comunication IP/10/1462 Brussels, from November, 4th 2010, to set out the strategy to strengthen EU data protection rules, available at: http://europa.eu/rapid/press-release_IP-10-1462_en.htm and then, Comunication IP/12/46, from January, 25th,2012 , to set out a comprehensive reform of data protection rules to increase either users' control of their data either to cut costs for businesses, available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm . - both, last access September2016.

6 Available at: http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN . It is also worth mentioning that on the same day were published **Directive(EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free

online, «*privacy by design*, *privacy by default»,* began to be valued *ab initio*, emphasizing the need for planning, construction, and development of a more *close-to-the-person* technological tools/objects. Never as now, privacy and security issues, protection of personal data - directly involving, first and foremost, the current user of the technological tool/object - are essential features in the R & D component of any organization who wishes to make any technological object available to the public. If there is some sort of an advantage in the *daily* discussion of the theme "*privacy*", it expresses itself precisely over this concern - either from the person either from organizations - regarding security (at least, some) and data protection. Although short on its ultimate purposes, since we insist that the focus should be always on people and not so much on their data, we can not neglect this positive effect of (some) *dual* awareness.

The present revolution, also dubbed *the Fourth Industrial Revolution or Industry 4.0, seems to have the potential to catapult our greatest dreams. But also most of our nightmares*. Klaus SCHWAB[7], for instance, puts the focus on the right premise, in all its essence: we must *«(...)"shape a future that works for all by putting people first, empowering them and constantly reminding ourselves that all of these new technologies are first and foremost tools made by people for people."».* Necessarily present, we find the Kantian maxim of the ideal of the human person as the first and last end of all things in such a premise. As a matter of fact, the only way society evolves is by not forgetting its origins: all its human essence.

Of course, we can not accept that technology presents itself to us as an exogenous force over which people have no control. Not for one single moment. First of all, technology derives from the person. Secondly, technology must be exclusively at the service of the person. And finally, technology should only complement the needs of the person. *By people, for the people*.

movement of such data, and repealing Council Framework Decision 2008/977/JHA, as well as **Directive(EU) 2016/681** of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. - last access September2016.

7 Available at: https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab/ , and https://www.project-syndicate.org/commentary/fourth-industrial-revolution-human-development-by-klaus-schwab-2016-01 . - last access September2016.

Concomitantly, in this relationship, the person can never be self-limited to that binary proposition (*so computer code*) in her choices, between 0 (zero) and 1 (one), between acceptance or rejection. Take the consecration of the right of access to the network as a human right[8]. By allowing the exercise of many of one person's civic rights in a quite similar way in the virtual world, thus, for example, electronic voting; delivering the income tax statement on the portal of the national tax authority; as well as many of the other connections that the person is establishing with a public administration in a increasingly digital state; the right of access to the network as a human right is presented as a logical result of the need to put technology at the main service of the person. Going a bit further, emphasizing the position assumed by the German Constitutional Court, terse on the case-law « BvR 370/07 *zum Urteil des Ersten Senats vom 27. Februar 2008*[9]*»*, the Court recognised as one fundamental right, the right to the integrity and confidentiality of information technology systems - *«Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme».* In such a landmark ruling, besides promoting user confidence, it sought to demand the State - as one of its tasks - to ensure the "*confidentiality*" and "*integrity*" of its information technology systems. The State must ensure (at least, try) our digital protection, safeguarding our *digital existence*.

This *new normal*, these new paradigms of life in society, involve risks. Naturally. Concerning it, we focus, in particular, on a right of each person to exercise control over the personal information concerning her. The excesses and /or abuses, derived from misuse of information, of databases, motivated either by negligence, inability, or by a distorted, false or discriminative individual, organizational, or state practices, cause us

8 UNITED NATIONS HUMAN RIGHTS COUNCIL (UNHRC). *THE PROMOTION, PROTECTION AND ENJOYMENT OF HUMAN RIGHTS ON THE INTERNET*. (2016) 32ND SESSION, 30 DE JUNHO. http://www.ohchr.org/EN/Pages/Home.aspx . - Last access September 2016.

9Available (in german language) at: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html . - last access September2016.

«Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen..»

greater concern. Sharpened by a *novel* reality of online, cloud, and big data computing. In reflection, is there a way to achieve the effective protection of the person and her personal data in this new social paradigm?

We tried to trace, in the present investigation, the more relevant - in our view, in a historical contextualized path – concepts and definitions regarding personal data and data protection. Seeking to clear the way for the construction of a right to informational identity, we went back to the 1980's, to the OECD *Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data.* From Convention 108, and its definitions, we've then scrutinized the contact points between the European Charter Of Fundamental Rights (*The Charter*) and the Data Protection Directive (*DPD 95/46/EC*). From Article 7 of the Charter, which states that "*Everyone has the right to respect for his private and family life, his home and his communications.*" and Article 8, where "*All persons have the right to the protection of personal data concerning them.",* being such data *"subject to fair treatment, for specific purposes, and with the consent of the person concerned or on other legitimate grounds provided for by law;"* to the model of legal principles and rights established in the Data Protection Directive – which we've reviewed in some detail, either from principles underlying the processing of personal data and principles relating to the quality of such personal data, to the guarantee function and intrusive legitimacy in fundamental rights covered by it – we've tried to lay down foundations for this right we pursue. Later and nevertheless, even if the objectives, principles and rights of the Directive remained valid, they haven't prevented the fragmentation of the its application at one common European level. Therefore, as result of a poignant jurisprudence of the CJEU, and one proposal for data protection reform in the European Union, the distance to a new legislative package of privacy, was an *apex*.

Seeking to fulfill the purpose of analyzing in an effective way the new european General Data Protection Regulation (*GDPR*) – Regulation E.U 2016/679[10] , in the course of the research, we have tried to take into account the new corollary of rights and guarantees which the new instrument seeks to crystallize in the European regulatory framework. Between a more demanding regulatory framework for organizations and a more guaranteeing context for people, analyzed in detail the Regulation, we are convinced that

10 Available at: http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:32016R0679&from=en . - last access September 2016.

it lends itself to refocusing the whole discussion of the personal data and data protection subject, closer to the person. Even if the context is, in advance, a glimpse of the single digital market for Europe, we believe that, when it comes into force in May 2018, there will be a greater awareness of the rights (and duties) that compete with people. As well as to organizations by addition. It will be in this context of mutual awareness, that future challenges concerning the relationship between person, technology, and law will unfold. Does the Regulation provide a sufficient instrument to better protect people in such a demanding online context? Sadly, it is an interjection that we still can not answer. As mentioned before, it is an exercise of prognose difficult to materialize. Above all because the Regulation only comes into force in May 2018. In any case, the prospects arising from the analysis of the regulation make us a bit optimistic. Without wanting to forget the movement of consecration of a *netizens Bill of rights*[11], we are convinced that the current picture may not be as dystopic as the some try to paint it.

Last, but not least, although this was not the order of exposure we've followed, we analyze in some detail the Portuguese national context, in constitutional and legal terms, bringing to the collation the relevant constitutional framework for the adoption of a right to informational identity. We've studied also some CNPD (the portuguese national supervisory authority) Doctrine, related to Sensitive Data, in particular, Opinions N. 28/2016 and 36/2016. In order to carry out the study, we've found that the solution may include the addition to the constitutional list of the rights freedoms and guarantees - in one future constitutional revision – from one right to informational identity, rooted in the express consecration, in Article 35, of the Portuguese Constitution (from now, CRP), of the right of access of the holders, as well as the rights of rectification and updating, the right to know the purpose of the processing of personal data. From this power/duty of control of personal data, contained in this constitutional support of article 35 together with the nature of freedom contained in article 26 number 1 of the CRP, once arrived, it should be granted the greater instrument of effective protection of personal data, the right to informational identity.

Still, we needed to highlight some perplexing curiosities regarding one – another – Portuguese authority – C.A.D.A - , which regulates access to administrative documents. Starting from a quite *sui generis* notion of personal information, a very poorly drafted

11As Sir Tim BERNERS-LEE, proposed it, and available at: https://www.ted.com/talks/tim_berners_lee_a_magna_carta_for_the_web . – Last access September 2016.

law[12], and one arrogating *exclusive competence*, this entity has been over the years producing obtuse *doctrine*. We will, only, bring Opinions 113/2015 and 36/2016 to stage. Fortunately, in August 2016, the legislator decided to put an end to all this legal *fog*. Once the new law[13] has been published, this entity – C.A.D.A. - inflected the doctrinal positions taken so far, as the Opinion 425/2016 will prove it.

Finally, still in the Portuguese context, we've highlighted, the successive and growing legal provision of access and interconnection from varied silos of data held by the public administration with the one owned by the Portuguese Tax authority. Punching, for instance, the constitutionality of the principle of purpose set out in Article 35 of CRP, neglecting the constitutionality tests of Article 18 of CRP, the Portuguese legislator is pushing to gather all the databases of the public administration into the giant silo of the AT (tax authority). As if the knowledge held by this authority was not already (almost) *complete*, the state has sought to institute it legally, seeking to emphasize the primacy of tax law over citizens' rights, freedom and guarantees, as if only tax law is only what matters. Thus the Portuguese state is pushing the American FATCA, thus the Portuguese state is broadening the vast competence of AT. And this set of unconstitutional intrusions goes lightly in the *Polis*. None of the governance political parties raise any particular questions. In fact, in a country with limited resources and anemic economic growth, only an *efficient* collection of income through taxes is able to balance the exiguous annual state budget. Hence it is *economically and efficiently* rational(is it?) that citizens shall be present to state bereft of *secrets*. One paternalistic state, devoid of space for secrecy, confidentiality or secrets, *taking care of all of its vitreous citizens* as equals. Such a totalitarian vision culminates in one *security* paradox: to pursue the state in the future, full vitracity. In the name of the *almighty* tax law, because there is no other way for economic growth, people have to present themselves stripped of secrets so that the paternalistic state takes care of all of them as *equals*. Here lies the foundation of maintaining our state for generations to come. Does it? Really?

12 The Law, is the *older* 2007 version of the Law on access to administrative documents (in Portuguese, L.A.D.A).
13 The new L.A.D.A, as the Law on access to administrative and environmental information and re-use of administrative documents, published in August 22th, 2016.

As a matter of fact, *who controls the controllers*? *Who watches the watchers*? The *algorithmic divinities* are here (as the ones who control the AT giant personal-data silo). They present themselves as the *only* instruments for treatment and/or storage, as well as for controlling activities of collection, cataloging, making available and conservation of personal data. The tool is using human as metrics. Even if the tool is fed by machine learning. Even so, there must be human control over these *divinities*, because these *deities* are – or at least, should be - exclusively at the service of the person. Not to use them. Always, *by people for the people*. Unfortunately the *state of the art* is trying to sediment one controlling technological reality over the *art of the states*. In fact, what would be the effective constitutional guarantee of protection - if any - if the technological *divinity* were to be the first to violate it? And only a few seems to care?

The technology that complements our natural human dissatisfaction should be exclusive to the person and not quite the opposite. In the end, we shall not forget this: The human being is not, nor can be, a mere informational object. Never. The human being is one end of human dignity.

1. SUMÁRIO

A sociedade global em rede da informação e do conhecimento, feliz no seu propósito de divulgação de múltiplas formas de conhecimento e de como lhe aceder, apresenta-se infeliz na sua compreensão da pessoa humana como um fim em si mesma. Não raras vezes toma-a como um "*mero objecto de informações*", usando e abusando dos vestígios informacionais que a pessoa vai colocando na rede. Se os vestígios compõem múltiplas partes de um só *todo*, é este *todo*, na qualidade da pessoa titular delas, que deverá poder controlar, sem constrangimentos, o caminho que lhes quiser emprestar. É, por exemplo, isso que se encontra expresso na conjugação dos *artigos 35.º e 26.º da CRP, abrangendo as posições jurídicas que se expressam desde a protecção da informação pessoal até ao livre desenvolvimento da personalidade.* É na identidade que o radical deve estar sempre focado. Na pessoa, no seu todo. Não nas "*partes informacionais*" com que o estado da arte o *divide*, e a arte dos estados por vezes a isso poderá induzir.

Palavras-chave: Direito a uma Identidade Informacional; Direito a ser Esquecido; Pessoa Humana; Dignidade Humana; *Algoritmocracia*

ABSTRACT:

The global society of the information network and knowledge, fortunate in its purpose of dissemination of various forms of knowledge and how to access it, seems to dismiss itself from understanding the human person as an end in himself. Too often it takes the human person as a "mere information object" using and abusing of some informational traces that we leave behind online. If one understands that these traces comprise multiple parts of a single *whole*, then it must be this *whole* the one that should be able to control without constraints, the action he wants to give them. This is what arises from the combination of Articles 35 and 26 of the Portuguese Constitution, covering all the legal positions that are expressed from the protection of personal information to the free development of personality. It is over the identity that the radical should always be focused on. In the person, as a whole. Not in the "*informational parts*" in which the *state of the art* divides the *whole*, or the *art of states* sometimes it may induce.

Keywords: Right To An (*online*) Informational Identity; Right To Be Forgotten; Human Person; Human Dignity; *AlgorithmCracy*

2. INTRODUÇÃO

No presente, na era da sociedade global da informação[14], a imparável evolução dos sistemas de comunicações electrónicas, a comunicação global em rede, *a Internet em todo o lugar a toda a hora*, a recolha, captura, anexação, indexação e transmissão em massa de *Big Data,* repletos de informações pessoais, identificáveis ou susceptíveis de identificar uma pessoa singular, obrigam a reformular toda a discussão em torno dos *dados pessoais e da sua protecção.*

A tónica da discussão tem estado apenas focada em *datum e na sua protecção*, em pacotes, *strings*, ficheiros e bases de dados e não no substancial de tudo isso, *i.e.*, nas pessoas. Ademais a *tentadora sedução*, pelo *comodismo, facilidade, imediatismo e disponibilidade da pesquisa informacional e dos seus resultados* (o cardápio argumentativo relativo a esta tentação será sempre muito profícuo), de transformação da pessoa em mero objecto informacional urge recentrar o debate em torno da protecção da pessoa, num tempo em que os valores primaciais do estado de direito democrático denotam já um grau de erosão difícil de combater. Assinalada a "*falha original*" (da doutrina de protecção de dados), cumpre superá-la, arrancando da dignidade humana, centrando-se em torno da "*informação pessoal*", positivando um adequado direito à identidade informacional.

2.1. METODOLOGIA E MÉTODO

2.1.1. O Problema

O objecto da nossa investigação, desde logo, apresenta-se-nos de difícil concretização. Arrojado nos propósitos. O Regulamento geral de protecção de dados europeu, o Regulamento 679/2016, sobre que discorreremos – com relativa profusão – apenas entrará em vigor nesse *longínquo* Maio de 2018. É um tempo demasiado longo para a velocidade assíncrona do tempo da tecnologia. Não obstante, estando já em curso o período de adaptação à nova moldura jurídica europeia, as questões centrais, em nosso

14 Secundamos Oliveira ASCENSÃO, quando a expressão, mais das vezes usada, «*sociedade da informação*», na verdade, corresponde a um mero *slogan*, defendendo, em sua substituição, a utilização de "*sociedade da comunicação*"- ASCENSÃO, Oliveira (2001) *Estudos Sobre Direito Da Internet E Da Sociedade Da Informação,* pp.163-164.

entendimento, ante a presente ou nova realidade tecnológica parecem-nos intemporais. Neste sentido, de seguida, poderíamos elencar as seguintes:

a) No presente, ante a emergente e pungente realidade de *big data*, a gigantesca massa de informação que circula e que se transmite na rede, até que ponto coartará o direito a uma identidade informacional da pessoa?
b) O direito a informar; a ser informado; a aceder ao conhecimento, a transmiti-lo e a partilhá-lo; à liberdade de opinião e de expressão e demais liberdades pessoais; à segurança; apenas conhecerão um movimento unidirecional, apontando no sentido do *mito* – que se vai cristalizando - de que *a internet nunca esquece*?
c) É a pegada digital que vamos deixando, em cada contacto que estabelecemos na rede e pela rede, assim tão impossível de *desindexar, apagar, deixar de rastrear, controlar*?
d) O direito ao esquecimento - algo tão humano como perdoar e esquecer - está assim tão dependente da factorização, métricas e de vontades algorítmicas que vão regendo e controlando a rede?
e) Teremos o direito a um arrependimento futuro sobre aquilo que concretizarmos no presente, na rede? Teremos o direito a ser deixados em paz, a não sermos importunados, mesmo mantendo uma fruição diária da rede? Ou só o conseguiremos afastados desta? Até quando será sociavelmente tolerável que o nosso passado assombre o nosso presente no mundo virtual?

2.1.2. Exposição do problema:

a) Nunca será fácil, perante uma exposição tão abrangente de motivos e temas, fazer um estreitamento singular da razão que nos move nesta investigação. A forma simples e sucinta como elencamos alguns aspectos supra, porém, permitem delinear um dado sentido da presente investigação. Naturalmente que esta, pressuposta de antemão na valoração da dignidade humana - realidade que nunca poderíamos prescindir - gravitará em torno do direito à identidade informacional e dos consequentes direitos intrincados na dignidade humana que nos caracteriza.
b) De facto, como procuraremos explicar, a imposição presente de um controlo e gestão da rede pelo *divino algoritmo* tem ensombrado – muito pela cristalização desse mito urbano de que a internet nunca esquecerá – a concretização, no virtual, de características tão humanas como esquecer, ser deixado em paz, o

arrependimento, perdoar. Todas estas características que compõem realidades fácticas mundanas, quotidianas, tão nossas. Que no entanto, têm apresentado resistências diversas à sua concretização na rede, no virtual.

c) Uma plena fruição e gozo destes direitos, humanos, contende – pelo menos em aparência – com as fórmulas de codificação usadas para a construção, dispersão e continuação da rede. Notando uma fragilidade na exposição deste motivo em concreto, não deixa de ser sintomático que, apenas recentemente e muito por culpa de uma jurisprudência do TJUE contundente, complementada agora por um Regulamento Geral de protecção de dados europeu, comecem a ser valoradas – pelo menos de forma diferente – a necessidade de planeamento e construção de objectos tecnológicos *mais amigos das pessoas*. *I.e.,* nunca como agora, preocupações quanto a questões de segurança, da própria privacidade, da protecção dos dados das pessoas - que envolvam directamente, e em primeiro lugar, o utilizador corrente do objecto tecnológico - naquela expressão anglo-saxónica de *privacy by design*, *privacy by default* são confirmadas logo na parte R&D de qualquer organização que se preste a querer colocar um qualquer objecto tecnológico à disposição do público.

d) Concomitantemente, em reflexão, só desta forma se poderá almejar à concretização de uma protecção eficaz da pessoa e dos seus dados pessoais. De facto, de que valeria a garantia constitucional de protecção se o objecto tecnológico se assumir como o primeiro a violá-la?

e) A consagração de forma expressa, no artigo 35.º, da CRP, do direito de acesso dos titulares, bem como dos direitos de rectificação e actualização, e ainda do direito a conhecer a finalidade do tratamento dos dados pessoais, apenas poderá conhecer concretização fáctica no mundo virtual se for acompanhada de mecanismos de segurança da privacidade tecnológicos próprios. Caso contrário, toda aquela discussão jurídica em torno da necessidade de uma *Bill of rights para os netizens*[15], estará, necessariamente, condenada ao fracasso.

15 Proposta avançada pelo inventor do www, Tim BERNERS-LEE, que poderá ser vista em: https://www.ted.com/talks/tim_berners_lee_a_magna_carta_for_the_web . – Último acesso Set.2016.

2.1.3. Justificação do problema:

A revolução presente, também apelidada de *quarta revolução industrial ou Indústria 4.0*, parece ter o condão para catapultar os nossos maiores sonhos. Mas também os pesadelos. Alinhamos com Klaus SCWAB[16]. A sociedade, como um todo, apenas poderá moldar um futuro melhor se mantiver sempre presente o ideal da pessoa humana como primeiro e último fim de todas as coisas.

Não poderemos, naturalmente, aceitar que a tecnologia se nos apresente como uma força exógena sobre o qual as pessoas não dispõem de qualquer controlo. De todo. Desde logo por que a tecnologia deriva da pessoa. E a pessoa, nesta relação, nunca se poderá apresentar autolimitada nas suas escolhas àquela proposição binária – tão característica da linguagem informática – entre o 0(zero) e o 1(um), entre a aceitação ou a rejeição. Pelo contrário. Qualquer decisão que tomarmos, naquela nossa base diária normal, individual e/ou colectiva, enquanto cidadãos livres, servirá de mote para orientar todo o rumo que quisermos emprestar ao progresso tecnológico. Porque este depende daquele(s), são as nossas escolhas, livres, que determinam o nosso futuro. E o da tecnologia que nos complementa as nossas naturais insatisfações humanas.

O *novo normal*, os novos paradigmas da vida em sociedade, envolvem riscos. No que concerne à presente investigação, focar-nos-emos, especialmente, num direito à identidade informacional, encerrando um direito de cada pessoa a exercer controlo sobre a informação pessoal que lhe diz respeito. São, por exemplo, os excessos e/ou abusos, derivados de um *mau uso* de informações, motivados por incúria, inabilidade, ou por uma distorcida, falsa ou discriminativas práticas individuais, organizacionais, ou estaduais, de bases de dados que nos causam maior preocupação. Mais ainda, em presença de uma realidade de computação em linha, da *cloud*, e do *big data*.

O poder/dever de controlo dos dados pessoais, constante desse respaldo constitucional do artigo 35.º, da CRP, definindo-se os limites dentro dos quais poderá ser desenvolvido, especialmente quando feitos por *divindades algorítmicas*, o tratamento e/ou

16«(…)*"shape a future that works for all by putting people first, empowering them and constantly reminding ourselves that all of these new technologies are first and foremost tools made by people for people."»,* disponível em: https://www.weforum.org/pages/the-fourth-industrial-revolution-by-klaus-schwab/ , e https://www.project-syndicate.org/commentary/fourth-industrial-revolution-human-development-by-klaus-schwab-2016-01 . - Último acesso Set.2016

armazenamento, bem como as actividades de recolha, catalogação, disponibilidade e conservação desses dados, estará na plena disposição do seu titular?

2.1.4. Alcances e limites da presente investigação

A investigação que propomos procurará dissertar, com especial relevo, sobre o *novo* contexto de protecção de dados introduzido pelo Regulamento U.E. 2016/679[17] e a relação que este instituirá – após a sua entrada em vigor – com cada cidadão e/ou organização. A história, jurídica, que culminou neste grande marco legal europeu será igualmente objecto de apreciação crítica. Naturalmente, cumpre salientar que perscrutaremos as realidades constitucionais e legal portuguesa, sendo estas – a par da realidade europeia – as balizas jurídicas da nossa investigação.

2.1.5. Objectivos gerais e objectivos específicos:

a) Como objectivos gerais - Derivada da jurisprudência recente do TJUE, mormente os Acórdãos *Google Spain* e o da revogação do *Safe Harbour agreement*, e da recente legislação europeia quanto à temática da protecção de dados, determinar se o novo RGPD (REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27/4) se constitui como marco suficiente para a protecção dos dados pessoais;

b) Como objectivos específicos - Perscrutar instrumentos de protecção efectiva dos dados pessoais, desde logo, delinear o direito à identidade informacional.

17 REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).* Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT – último acesso Set.2016

2.2. OPÇÕES BIBLIOGRÁFICAS

Pelo presente, sublinhamos que, na composição da presente investigação, o mote das escolhas bibliográficas que fizemos, procurou encontrar abrigo em muita da informação disponibilizada sem constrangimentos autorais, ou seja, de livre acesso. Não menosprezando as querelas jurídicas que se vão instando através das premissas subjacentes a direitos de propriedade, patentes e direitos de autor – que na presente investigação não relevam – tomamos a opção de, partindo da noção, pessoalíssima, de que o conhecimento e o acesso a este não deverão conhecer barreiras – pois que este é um direito humano que cumpre sempre defender - optarmos por dar maior primazia a uma bibliografia de fonte aberta, disponível, acessível, pesquisável através desta enorme ferramenta que é a internet. Reconhecemos, de antemão e sem margem para dúvida, note-se, o valor autoral e científico intrínseco de cada *investigação* que fomos lendo, investigando e estudando, nas suas variadas formas, seja por manuais impressos, seja por formatos digitalizados. Aliás, para compor a presente dissertação, só a consulta de segmentos variados de manuais, obras, Acórdãos, Legislação, notícias e reportagens - os quais fomos dando conta destes nas devidas notas de rodapé, e, de igual forma, na Bibliografia – permitiu chegar a este resultado final. O seu a seu dono. Naturalmente. Mas, à semelhança do projecto do qual fazemos parte e que vamos dando a conhecer noutras circunstâncias, a opção por um método que observe os termos e condições de uma ferramenta, como por exemplo e passe a publicidade, uma licença (*creative commons) CC 3.0*[18], com as possibilidades que tal encerra, foi deliberada e em consonância com as nossas convicções. "*Unleash the knowledge, and dare to share it"*, atreva-se a libertar e partilhar o conhecimento, a humanidade agradece(rá).

NOTA: NÃO NOS OPOMOS A UMA PARTILHA DO PRESENTE ESTUDO, DESDE QUE ESTA RESPEITE AS CONDIÇÕES DA LICENÇA CC 3.0.

18 *Vide* a propósito: https://creativecommons.org/licenses/by/3.0/pt/ - último acesso Set.2016

3. A PROTECÇÃO DE DADOS NO *PIONEIRISMO* JURÍDICO DO DIREITO EUROPEU

Hodiernamente, numa sociedade, tecnologicamente cunhada como sendo de informação ou do conhecimento, recheada de "*Nativos e imigrantes digitais*[19], a informação (e a *complexidade* dos dados que a suportam) possui um valor inelutável no quotidiano dos Estados, das Organizações e das pessoas singulares (cada vez mais enquanto *netizens*). Ante o paradigma actual tecnológico e perante o disruptivo poder de processamento dos dados e de computação em linha, a superação *Orwelliana* de uma sociedade moldada em torno de um *Big Brother* assume-se presente na nossa base diária de vida em sociedade. O "*eu*", transportado por vastas bases de dados digitais, dispostas em variadas proveniências, torna-se acessível por múltiplas organizações e indivíduos e objectos tecnológicos, à distância de um mero clique ou toque[20]. Um "*eu*" diáfano, *objecto* de segmentações e propósitos variados, relativizado numa mera *string* de *bits*. É, precisamente, no contexto desta revelação (provocatória e que queremos neutralizar), postulando a salvaguarda *da identidade informacional* da pessoa, da sua privacidade *online*, enquanto *indivíduo globalizado e globalizante*, e da sua protecção dos dados pessoais – de múltipla natureza –, que encontramos o objeto da presente dissertação.

Antes de partirmos, porém, cabe formular uma nota prévia, necessária. Na obra cardinal de WARREN e BRANDEIS, de finais do Séc. XIX, *the Right to Privacy*, os autores procuraram materializar um conceito de *privacy* arrancado de uma perspectiva de direito privado, de direitos muito próximos da defesa da propriedade, do direito de autor, *copyright* e do *Right to be let alone*. Naqueles tempos (1890), ante a profusão da fotografia instantânea, aliada a um sensacionalismo jornalístico *(«Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life ; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops"*»), os referidos autores procuraram materializar um conceito que, desde logo, obstasse à exposição das pessoas que pretendiam evitar a *public disclosure* americana, procurando

19 Juntando uma perspectiva interessante de confronto geracional que vai ocorrendo, também como na vida real, na rede virtual. MARK PRENSKY, DIGITAL NATIVES, DIGITAL IMMIGRANTES. disponível em: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf . último acesso Out.2016.

20 Basta recordar a multitude de aparelhos com acesso à rede. Desde computadores – em sentido latíssimo – a telemóveis inteligentes, híbridos e afins. Entre um clique e um toque no *touchscreen*, o mundo está à distância da nossa mão, onde a *velha* questão do "*polegar oponível*" caducou com a passagem deste tempo.

manter a sua vida privada e afastada dos olhares curiosos do público. Formalizando-o em torno desta problemática, os autores procuraram construir mecanismos de tutela jurídica da(quela) *privacy*, perscrutando a *common law*[21] ao encontro de bastiões de carácter cautelar. A *privacy* brotou, naquele contexto, como um argumento jurídico, relacionado com a defesa do direito do indivíduo de adopção das decisões *íntimas* que melhor lhe aprouverem, em harmonia com o seu *espaço sagrado da vida doméstica e privada*. Cumpre-nos salientar, de todo o modo, as seis (6) conclusões[22] com que, naquela época, surpreenderam o mundo: *«1.The right to privacy does not prohibit any publication of matter which is of public or general interest. In determining the scope of this rule, aid would be afforded by the analogy, in the law of libel and slander, of cases which deal with the qualified privilege of comment and criticism on matters of public and general interest;(...) 2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.(...) 3.The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage.(...)4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent.(...)5. The truth of the matter published does not afford a defence. Obviously this branch of the law should have no concern with the truth or falsehood of the matters published;(...) 6. The absence of "malice in the publisher does not afford a defence. Personal ill-will is not an ingredient of the offence, any more than in an ordinary case of trespass to person or to property.(...)».*

Na presença do actual nevoeiro, de profusão de significantes e de contextos, *privacidade, dados, protecção de dados*, será possível *orientarmo-nos no caminho*? Vamos por partes.

---

21 «*That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses* vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms ; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, — the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession — intangible, as well as tangible.» - WARREN, SAMUEL D., BRANDEIS, LOUIS D., The Right To Privacy, Originally Published In The Harvard Law Review, V. Iv, No. 5, December 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm* . – último acesso Set.2016.

22 *Idem. Op.cit.*

De que direito a uma *protecção dos dados de carácter pessoal que lhes digam respeito* e de que *tratamento* (dos dados pessoais) *concebido para servir as pessoas* falamos, quando relacionamos os *tópoi* ínsitos? Conseguiremos assentar o caminho jurídico rumo a um *direito a uma identidade informacional* [23] (PINHEIRO, 2015)?

Numa tentativa, tosca desde logo pelo movimento *world wide* que a matéria reclama, de delimitação do objecto do presente estudo, optaremos por conceder mais relevo a intrincadas questões europeias de *protecção de dados pessoais*. Por conseguinte, numa óptica de proximidade física, – insistimos, ainda que esta apareça comprometida quando perspectivada sob pressupostos de computação em linha – cumpre-nos destacar, neste breve excurso histórico, um *pioneirismo* europeu relativamente à protecção dos dados pessoais.

Assinalaremos, entretanto, o nosso ponto de chegada: o novo Regulamento geral de Protecção de Dados, o REGULAMENTO (UE) 2016/679[24] DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, doravante GDPR. Assim, precipitando, registamos que:

i) ««***Dados pessoais****», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*»[25];

23 Seguimos a posição de Alexandre SOUSA PINHEIRO: «(…) *o "património da protecção de dados" deve ser integrado num direito de maior latitude que designaremos como direito à identidade informacional. (...) o acquis de mais de 40 anos de labor doutrinário e jurisprudencial – vertido amiúde em instrumentos legislativos – não sofre perdas de sentido ou subtracção de posições jurídicas individuais, antes obriga à sua integração numa nova figura*.» - SOUSA PINHEIRO, Alexandre, *Privacy e Proteção de Dados Pessoais: A Construção do Direito à identidade Informacion*al? AAFDL: lisboa, LISBOA, 2015, p. 810.

24 REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). – disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT – Último acesso Set.2016

25 Artigo 4.º, n.º1, do GDPR.

ii) «*«**Tratamento**», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;*»[26].

Uma vez chegados a *bom porto*, que caminho desbravámos até alcançar alguma *estabilidade* destes conceitos nos nossos ordenamentos jurídicos?

3.1. OS ALICERCES JURÍDICOS DA CONVENÇÃO N.º 108 PARA A PROTECÇÃO DE PESSOAS SINGULARES

Perscrutando o trilho, *ab initio*, europeu, do *direito a uma identidade informacional,* cabe destacar a Convenção n.º 108 para a Protecção das Pessoas Singulares, no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981[27], adoptada pelo Conselho da Europa. Inspirada na matriz orientadora das «*Guidelines governing the protection of privacy and transborder flows of personal data*» de 1980[28] (revistas em 2013[29]) da Organização para a Cooperação e Desenvolvimento Económico (OCDE), a Convenção 108 despontou como o primeiro instrumento europeu juridicamente vinculativo adoptado no domínio da protecção de dados. Clarificando o seu propósito, logo no Preâmbulo, a Convenção propõe-se *alargar "a protecção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado; Reafirmando ao mesmo tempo o seu empenhamento a favor da liberdade de informação sem limite de fronteiras; Reconhecendo a necessidade de conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os povos"*. Neste conspecto, em conformidade com o seu artigo 2.º, são: «a) Dados de carácter pessoal - *"qualquer*

26 Artigo 4.º, n.º2, do GDPR.
27Disponível, por exemplo, em: http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhregionais/conv-tratados-28-1-981-ets-108.html - último acesso Set.2016
28https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm - último acesso Set.2016
29 https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf - último acesso Set.2016

informação relativa a uma pessoa singular identificada ou susceptível de identificação ("titular dos dados"; b) Ficheiro Automatizado – *"qualquer conjunto de informações objecto de tratamento automatizado";* c) "Tratamento automatizado" – "*as seguintes operações, efectuadas, no todo ou em parte, com a ajuda de processos automatizados: registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extracção ou difusão;*».

Em 1980, a realidade tecnológica *vivia a anos-luz* da *world wide web* idealizada por BERNERS LEE[30]. Sumariamente, nesses idos anos 80, do século passado, a rede (internet) estava circunscrita a militares (essencialmente americanos) e à academia[31] (alguma). Nichos, *desconectados*, à margem da rede de conexões mundial que hoje conhecemos e usufruímos. O *dilúvio informacional* sobre que hoje somos *surpreendidos instantaneamente na palma da nossa mão*, simplesmente, não existia. Não obstante, a Convenção denotou – certeiramente – a relação intrínseca, e intensa, que se iria constituir como *um novo normal*, a relação entre dados de carácter pessoal e o seu tratamento (automatizado e por via de ficheiros automatizados).

30 A ideia de Tim BERNERS-LEE, para a construção daquilo a que hoje acolhemos mundialmente como *world wide web* - «*Information Management: A Proposal*», disponível em: http://info.cern.ch/Proposal.html - último acesso Set.2016.

31 «*As the Web began to grow, Tim (Berners-Lee) realised that its true potential would only be unleashed if anyone, anywhere could use it without paying a fee or having to ask for permission. He explains: "Had the technology been proprietary, and in my total control, it would probably not have taken off. You can't propose that something be a universal space and at the same time keep control of it."*». Um pouco da história da *worldwideweb* pode ser consultada em: http://webfoundation.org/about/vision/history-of-the-web/ - último acesso Set.2016.

3.2. DA CARTA EUROPEIA DOS DIREITOS FUNDAMENTAIS

Em 24 de Outubro de 1995, através da Directiva 95/46/CE[32] do Parlamento Europeu e do Conselho (doravante a DPD), surge um novo instrumento jurídico que assume um conjunto de obrigações e direitos baseados na própria Convenção, passando a reivindicar uma maior protecção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e respetiva livre circulação. A DPD vem assumir uma posição firme, *preditiva*, num contexto temporal em que o fenómeno da recolha, armazenamento, tratamento e transmissão de dados *apenas* começava a dar os primeiros passos. O *novo normal*, seguindo a arquitectura desenhada por BERNERS-LEE e que acabou por tomar conta das nossas actuais *vidas digitais*, contava apenas com cerca de cinco (5) anos de existência[33]. Pela importância que a DPD representa(*ou*), a ela regressaremos adiante.

Volvidos cerca de cinco (5) anos, e no seguimento de uma vontade política e transformações tecnológicas e sociológicas pungentes – que se iam *globalizando* -, a U.E. procurou instituir uma *Carta dos direitos fundamentais da União europeia*[34], atenta a reconhecida necessidade de reforçar a protecção dos direitos fundamentais dos seus cidadãos. Decorria a cimeira que instituiu o Tratado de Nice, em Dezembro de 2000 e, por razões e inaptidões jurídicas diversas que não relevam para o presente efeito, a *Carta*, *reponderada* assim como a própria estrutura da União, apenas seria vertida nos ordenamentos jurídicos dos estados-membros da U.E., nove anos mais tarde, *i.e.*, após a entrada em vigor do tratado de Lisboa, em Dezembro de 2009. De facto, o texto da Carta *retoma, adaptando-a, a Carta proclamada em 7 de Dezembro de 2000 e substitui-a a partir da data de entrada em vigor do Tratado de Lisboa*. Note-se ainda que a Carta dos Direitos Fundamentais, tendo-se tornado juridicamente vinculativa, em conformidade com o TUE[35], no seu artigo 6.º, passou, complementarmente, a ter o mesmo valor (e dignidade) jurídico dos Tratados europeus.

---

32 http://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A31995L0046 – último acesso Set.2016.
33 «*By October of 1990, Tim had written the three fundamental technologies that remain the foundation of today's Web (and which you may have seen appear on parts of your Web browser): HTML: HyperText Markup Language. The markup (formatting) language for the Web. URI: Uniform Resource Identifier. A kind of "address" that is unique and used to identify to each resource on the Web. It is also commonly called a URL. HTTP: Hypertext Transfer Protocol. Allows for the retrieval of linked resources from across the Web*.». *Vide* nota rodapé 8.
34 http://www.europarl.europa.eu/charter/pdf/text_pt.pdf - último acesso Set.2016.
35 TRATADO DA UNIÃO EUROPEIA (VERSÃO CONSOLIDADA), disponível em: http://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF – último acesso Set.2016

Aligeirando as vicissitudes políticas – que em nada motivam o presente excurso - não poderíamos, de todo, negligenciar a fundamentalidade da Carta[36]. Efetivamente, sufragando o princípio da indivisibilidade dos direitos fundamentais, a Carta assumiu a responsabilidade de romper com distinções e barricadas avulsas, entre direitos civis e políticos, de um lado, e direitos económicos e sociais, do outro. Ao enumerar e agrupar todos os direitos fundamentais em torno de valores e princípios-chave estruturantes da União, como os da dignidade humana, das liberdades fundamentais, da igualdade e solidariedade, dos direitos dos cidadãos e da justiça, a Carta alargou o escopo de protecção dos direitos fundamentais onde a própria União Europeia se funda[37], *reforçando a protecção dos direitos fundamentais, à luz da evolução da sociedade, do progresso social e da evolução científica e tecnológica.*

Enquanto instrumento jurídico vinculativo[38], na parte que mais releva para o presente estudo, chamamos à colação, entre outros, o artigo 7.º, que estabelece que *"todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.»,* bem como o artigo 8.º, o qual estipula, no seu número 1, que *"todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.",* devendo esses dados, em conformidade com este número 1, "*ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei."*. Por último, cabe realçar os direitos de acesso *"aos dados coligidos que lhes digam respeito"* e o da obtenção da *"respectiva rectificação"*, igualmente consagrados no sobredito artigo.

A Carta vincula as instituições e órgãos da União Europeia, os seus Estados-membros e ainda, os particulares, quando estes (e todos) apliquem o direito comunitário. Tratando-se de normas com eficácia directa[39], no âmbito das atribuições e competências próprias da União Europeia e de acordo com o princípio da subsidiariedade, a Carta deve ser interpretada *de acordo com as disposições gerais constantes do Título VII (da Carta) que*

36 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:PT:PDF - – último acesso Set.2016.

37 Artigo 2.º do TUE (versão consolidada): «*A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem, incluindo os direitos das pessoas pertencentes a minorias. Estes valores são comuns aos Estados-Membros, numa sociedade caracterizada pelo pluralismo, a não discriminação, a tolerância, a justiça, a solidariedade e a igualdade entre homens e mulheres.»*

38 Cfr. Artigo 6.º, do TUE.

39 Artigos 51 e ss da Carta,

regem a sua interpretação e aplicação e tendo na devida conta as anotações a que a Carta faz referência, que indicam as fontes dessas disposições. Em acréscimo, demanda o reforço de protecção europeia no tocante aos direitos fundamentais, em especial d*os direitos que decorrem, nomeadamente, das tradições constitucionais e das obrigações internacionais comuns aos Estados-Membros, da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais, das Cartas Sociais aprovadas pela União e pelo Conselho da Europa, bem como da jurisprudência do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem*, ora ampliando-o[40] ora, e/ou, reforçando-o[41] [42]. O que, obviamente, encontra fundamento na panóplia de competências, por exemplo, que se foram diversificando e inculcando no seio da estrutura da U.E., bem como todas as formas de cooperação em matérias de assuntos internos, de justiça, de matéria penal, cuja *praxis* – mesmo que potencialmente – tem gerado decisões susceptíveis de repercussões diversas nos domínios das mais elementares liberdades fundamentais das pessoas.

O padrão de protecção das pessoas e dos seus dados pessoais foi assertivamente contaminado pelo ambiente descrito de abundante generosidade jurídica para com os direitos fundamentais. Desde logo, a própria DPD acabou por ver reforçado o seu escopo de protecção dos dados pessoais, na senda da sedimentação na ordem jurídica europeia[43] de direitos fundamentais como os do direito à liberdade e à segurança (artigo 6.º), do respeito pela vida privada e familiar (artigo 7.º), da protecção dos dados pessoais (artigo 8.º), da liberdade de expressão e de informação (artigo 11.º), da liberdade de empresa (artigo 16.º), mas também, do direito de acesso aos documentos (artigo 42.º).

3.3. DA RELEVÂNCIA DA DPD NO TRILHO DA ESTABILIDADE JURÍDICO CONCEPTUAL

Pela nossa parte, no que concerne à DPD, cumpre salientar, mesmo que de forma perfunctória, os pontos seguintes:

40 Cfr. Artigo 52.º, n.º 3, parte final da Carta.
41 Artigo 53.º da Carta.
42 «*Nível de protecção - Nenhuma disposição da presente Carta deve ser interpretada no sentido de restringir ou lesar os direitos do Homem e as liberdades fundamentais reconhecidos,(...)*»
43 Através da Carta, em especial pelo seu Título II – Liberdades.

a) A DPD assumindo um conjunto de obrigações e direitos baseados na Convenção 108, passou a definir, no seu Artigo 2.º, que «*a) «**Dados pessoais**», qualquer informação relativa a uma pessoa singular identificada ou identificável (« pessoa em causa »); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social; b) «**Tratamento de dados pessoais**» («tratamento»), qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;*».

b) Em termos jurídico-positivos, notamos uma relevante e clarificadora evolução dos conceitos (por comparação com 1980), atenta as *imparáveis* novidades de cariz tecnológico. Por um lado, o conceito de dados pessoais viu a sua esfera de protecção estender-se, precisamente na parte, dúbia, ao que for *susceptível de identificação* como tal. Em termos proporcionais, a esfera protectiva do conceito de tratamento passou a prever, duplicemente, quer tratamento automatizado, quer tratamento não-automatizado (*vide* inclusive Considerando (27)), bem como uma definição mais precisa da ambiguidade *das operações lógicas e ou aritméticas* efectuadas *com a ajuda de processos automatizados*.

3.3.1. DO MODELO PRINCIPIOLÓGICO DA DPD

No que concerne aos respetivos princípios norteadores, a DPD[44] funda-se em dois grandes grupos de princípios: os que **fundamentam o tratamento de dados pessoais** e os princípios **relativos à qualidade dos dados pessoais.**

3.3.1.1. Quanto ao primeiro bloco, pretendemos salientar, por um lado, um **princípio** (geral) **da transparência**, transversal a qualquer relação, jurídica ou

44 Assinalando a base jurídica conferida pela Convenção, e o seu articulado no Capítulo II, mormente artigos 5.º e 6.º.

não. Partindo, por exemplo, dos Considerando 25 e 26[45] da DPD, este princípio da transparência postula um conjunto de obrigações e garantias a observar pelas entidades nele destacadas, bem como um conjunto de direitos afectos às pessoas singulares, atinentes aos dados pessoais e respectivo tratamento. Veicula-se, primacialmente:

a) Através dos direitos fundamentais à informação - em sentido lato, um direito de amplo espectro[46], de acesso[47] e de oposição[48];

b) Nas garantias fundamentais institucionais vertidas na segurança do tratamento[49] e no dever e conteúdo da notificação para registo ou autorização das Autoridades Nacionais de protecção de dados[50].

O que, escalpelizado, nos permite aferir que sendo, por natureza, indissociáveis "transparência" e "protecção", e constituindo-se ambas como características inatas de um qualquer processo de tratamento de dados, o princípio da transparência demanda – certeiramente – a indicação de forma verdadeira, manifesta e lícita, e nunca meramente enunciativa, do conteúdo da finalidade. *Cardinal*[51], com feito, este **princípio da finalidade** (da sua especificação e da sua limitação), insta a que os dados só possam ser

45 *«(25)Considerando que os princípios de protecção devem encontrar expressão, por um lado, nas obrigações que impendem sobre as pessoas, as autoridades públicas, as empresas, os serviços ou outros organismos responsáveis pelo tratamento de dados, em especial no que respeita à qualidade dos dados, a segurança técnica , à notificação à autoridade de controlo, às circunstância:, em que o tratamento pode ser efectuado, e , por outro, nos direitos das pessoas cujos dados são tratados serem informadas sobre esse tratamento, poderem ter acesso aos dados, poderem solicitar a sua rectificação e mesmo, em certas circunstâncias, poderem opor-se ao tratamento;»* e, *«(26)Considerando que os princípios da protecção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável ; que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa , para identificar a referida pessoa ; que os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável; que os códigos de conduta na acepção do artigo 27 podem ser um instrumento útil para fornecer indicações sobre os meios através dos quais os dados podem ser tornados anónimos e conservados sob uma forma que já não permita a identificação da pessoa em causa;»*

46 Artigos 10.º e 11.º.

47 Artigo 12.º.

48 Artigo 14.º.

49 Artigo 17.º.

50 Artigos 18.º e 19.º.

51 «(…)*constitui o princípio verdadeiramente cardinal da protecção de dados, sendo essencial a definição precisa destas finalidades, sendo os demais princípios função deste na medida em que os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade pretendida; devem ser exactos, completos e actualizados em função da finalidade; e só devem ser conservados pelo tempo que a finalidade exige. Por outro lado, a finalidade assume também relevância no momento em que é assegurado o direito à informação nos termos do art. 10.º, n.º 1, da Lei de Protecção de Dados Pessoais, assim como no momento em que a autoridade de controlo vai apreciar os pedidos de autorização ou de notificação dos tratamentos de dados pessoais.*», COELHO MOREIRA, Teresa, "O Controlo Electrónico dos Emails dos Trabalhadorers", *in Congresso Iberoamericano de Derecho Informático*, 2011, p. .5.

utilizados para a finalidade *determinante* da recolha, sendo que a mesma deve ser *determinada, explícita e legítima* antes do início do tratamento[52] Valendo como um *"princípio de proibição"*, revela-se enquanto princípio *fiscalizador da legitimidade do tratamento*, *garantindo por um lado que a recolha de informação não é "cega" às suas consequências e que, dentro de um determinado tratamento de dados, a recolha seja limitada aos elementos necessários para a prossecução da finalidade*[53].

3.3.1.2. Por outro lado, no que concerne ao segundo bloco, onde se alojam os **princípios relativos à qualidade dos dados** – *ex vi*, por exemplo ainda, Art.º 5.º da Convenção - denotamos um traço comum[54], distintivo, intrinsecamente ligado ao princípio da finalidade. Neste contexto, cumpre-nos destacar:

a) O **princípio da licitude e do tratamento leal** - trata-se de um princípio pressuposto no princípio da transparência, e apressado no consentimento[55], objectivando que o tratamento de dados pessoais não deverá, em caso algum, ocorrer por *razões secretas*, devendo ser cotejado pela verificação do cumprimento das regras jurídicas nacionais, europeias e internacionais (*ad substantiam* subordinado aos princípios gerais do direito, mormente, ao princípio da boa fé), nos termos do artigo 6.º, n.º1, alínea a).

b) O **princípio da adequação, pertinência e proporcionalidade** – o qual postula que os dados pessoais tratados têm de ser adequados à finalidade para que são recolhidos. Obviamente. Uma vez tratados, a sua qualidade deve ser idónea para as finalidades daquele tratamento, mostrando-se ainda pertinentes relativamente às finalidades enunciadas. As baias da proporcionalidade impõem ainda que o tratamento não possa ser excessivo, i.e., não ultrapasse o necessário para a finalidade do tratamento proposto, conforme a alínea c), do número 1, do artigo 6.º.

c) O **princípio da exactidão e actualização dos dados** – reclama que os dados devem ser exactos e, se possível, actualizados[56] exigindo-se que, quer um, quer outro, sejam, igualmente, aferidos em função da finalidade do tratamento de dados e que,

52 Artigo 6º, n.º1, al. b).
53 SOUSA PINHEIRO, Alexandre, *Op.cit.* p. 806.
54 «*Considerando (28) que qualquer tratamento de dados pessoais deve ser efectuado de forma lícita e leal para com a pessoa em causa; que deve, em especial, incidir sobre dados adequados, pertinentes e não excessivos em relação às finalidades prosseguidas com o tratamento; que essas finalidades devem ser explícitas e legítimas e ser determinadas aquando da recolha dos dados; que as finalidades dos tratamentos posteriores à recolha não podem ser incompatíveis com as finalidades especificadas inicialmente.*»
55 *Vide* «Considerando(30) (…) *para ser lícito, o tratamento de dados pessoais deve, além disso, ser efectuado com o consentimento da pessoa(...)*».
56 Artigo 6.º, número 1, alínea d).

sucessivamente, na impossibilidade de rectificação ou actualização – seja, por exemplo, porque os dados se apresentem já desfasados em relação ao tempo, seja porque perderam conexão com a finalidade com que foram recolhidos - sejam apagados.

d) O **princípio da limitação da conservação dos dados e da sua derrogação para fins estatísticos e de investigação científica -** constante do Art.º6.º, n.º1, al. e)), que se postula como uma espécie de *excepção*[57], limitada nos seus propósitos, mas obrigando os Estados-membros a adoptar legislação interna com as necessárias garantias, adequadas, contra a utilização indevida, salvaguardando a privacidade individual dos seus cidadãos.

e) O **princípio da responsabilidade** - insíto no número 2 do Artigo 6.º. Cogente, incumbe ao responsável[58] pelo tratamento dos dados o cumprimento e a observância dos princípios enumerados, como garante da (inter) operabilidade destes.

Como será óbvio de constatar, qualquer que seja a modalidade de tratamento de dados pessoais – recolha, armazenamento, processamento, modificação, transferência ou apagamento –, o mesmo deverá ser perspectivado, aprioristicamente, como uma intromissão nos direitos fundamentais da pessoa. Não havendo direitos absolutos, nem absolutistas, esta intrusividade reclama, necessariamente, uma dada legitimação. Uma vez elucidado o modelo principiológico da DPD, cumpre-nos evidenciar a respectiva vertente garantística, nomeadamente em sede de direitos fundamentais - sempre na óptica dos dados pessoais das pessoas singulares - nas tensões que o confronto destes com o tratamento dos seus dados provoca, casuística e/ou potencialmente. A DPD apresenta a lei e um – *deficiente* - consentimento como fundamentos de legitimidade.

57 Perfilhamos a ideia de Catarina SARMENTO E CASTRO. «*Parece à primeira vista, uma excepção ao princípio da limitação da conservação dos dados pessoais ou ao direito ao esquecimento. Mas não é: apenas se passa a admitir que os dados passem a ser tratados para fins históricos, estatísticos ou científicos, quando estes não sejam considerados incompatíveis com os fins do tratamento original.*» - *Direito da Informática, Privacidade e Dados Pessoais*, 2005, Almedina: Coimbra, p.. 241.

58 Secundamos as interjeições postas em evidência pelo *«"Memorando explicativo da Comissão" - Protection of Personal Data, Select Committee on the European Communities, 1992-93, 20th Report, p.61»*, *apud*. SOUSA PINHEIRO, Alexandre, *op.cit.,* pp.610-611. Com efeito, « *O perigo de processos de decisão baseados em tratamentos de dados inadequados pode constituir no futuro um problema, o maior problema, no que respeita ao uso de dados automatizados: o resultado produzido pelos computadores, recorrendo a software cada vez mais sofisticado, e a sistemas cada vez mais desenvolvidos, tem como consequência que o peso da responsabilidade da decisão passe do homem para o computador, abdicando aquele das suas responsabilidades.»*. Essencial, portanto, a conformação jurídica de *checks-and-balances* pressupostos no princípio da responsabilidade, sob pena de atropelos *automatizados* a direitos fundamentais.

3.3.2. DA FUNÇÃO GARANTÍSTICA DA DPD E DA *LEGITIMIDADE* INTRUSIVA NOS DIREITOS FUNDAMENTAIS

A legitimação poderá trajar-se de um consentimento[59] inequívoco do titular dos dados pessoais[60], fundado na necessidade de celebração de um contrato[61], de cumprimento de uma dada obrigação legal[62], de protecção de interesses vitais[63] do titular dos dados[64], ou em virtude de uma acção de interesse[65] e/ou autoridade[66] públicas[67].

A redacção propugnada pela DPD, pela sua *excessiva amplitude* relativamente ao **consentimento**, posiciona-se como alvo susceptível de críticas várias. De facto, a redacção da alínea f) do artigo 7.º abre a porta a um *interesse legítimo do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados* para, visando variadas transacções de carácter comercial, proceder ao tratamento desses dados pessoais. Esta interpretação, ainda que alegadamente *legitimada*, complementando uma *perversa redacção* - pelos pretextos que viabiliza ao iludir esta noção de consentimento enquanto uma manifestação da licitude do tratamento[68] - fere inequivocamente ainda o

---

59 *Vide,* por exemplo, «*Considerando (33) que os dados susceptíveis, pela sua natureza, de pôr em causa as liberdades fundamentais ou o direito à vida privada só deverão ser tratados com o consentimento explícito da pessoa em causa; que, no entanto, devem ser expressamente previstas derrogações a esta proibição no que respeita a necessidades específicas, designadamente quando o tratamento desses dados for efectuado com certas finalidades ligadas à saúde por pessoas sujeitas por lei à obrigação de segredo profissional ou para as actividades legítimas de certas associações ou fundações que tenham por objectivo permitir o exercício das liberdades fundamentais*.»

60 Artigo 7.º, alínea a).

61 Artigo.7.º, alínea b).

62 Artigo 7.º, alínea c).

63 *Vide* por exemplo, «*Considerando(31) que, do mesmo modo, o tratamento de dados pessoais deve ser considerado lícito quando se destinar a proteger um interesse essencial à vida da pessoa em causa;»*

64 Artigo 7.º, alínea d).

65 *Vide* por exemplo, «*Considerando(32) que cabe às legislações nacionais determinar se o responsável pelo tratamento que executa uma missão de interesse público ou exerce a autoridade pública deve ser uma administração pública ou outra pessoa sujeita ao direito público ou ao direito privado, por exemplo uma associação profissional;»* e *«Considerando(34) que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social — em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença — e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia,, estabelecer garantias adequadas e específicas para a protecção dos direitos fundamentais e da vida privada das pessoas;*».

66 *Idem*. E ainda, *vide* por exemplo, «*Considerando(35), além disso, que o tratamento de dados pessoais pelas autoridades públicas para a consecução de objectivos consagrados no direito constitucional ou no direito internacional público, em benefício de associações religiosas oficialmente reconhecidas, é efectuado por motivos de interesse público importante;*»

67 Artigo 7.º, alínea e).

68 *Vide,* por exemplo, novamente, «*Considerando (30) que , **para ser lícito, o tratamento de dados pessoais deve, além disso, ser efectuado com o consentimento da pessoa em causa** ou ser necessário para a celebração ou execução de um contrato que vincule a pessoa em causa, ou para o cumprimento de uma obrigação legal, ou para a execução de uma missão de interesse público ou para o exercício da autoridade*

princípio da transparência, nas suas dimensões de lealdade e boa-fé, na recolha de dados pessoais. Importa reforçar que o "*eu*", em toda a sua multitude de facetas, não é um "objecto" vertido nem numa mera *string* de *bits*, nem num pacote de dados, nem num número de telefone[69].

Não podemos negligenciar que o espaço refinado do consentimento apenas fará sentido se o titular dos dados pessoais compreender o binário *razão+finalidade* da recolha dos seus dados. Efectivamente, *ex ante,* é manifesta a necessidade de vincar o espaço fulcral que a finalidade reclama. Esta, enquanto princípio, impõe-se ao consentimento. Precisamente por entender a necessidade de tutela das situações em que o consentimento esteja, pela natureza das coisas, limitado. Consentir é abdicar. *Abdicar de*, implica uma escolha. Esta escolha só poderá ser concretizada se a pessoa - que e quando a fizer - estiver na posse de toda a informação possível, para o fazer de forma racional. Destemida. Sem a invocação da razão-finalidade para que, em função dela, a pessoa possa determinar a natureza necessária (ou não) da informação pessoal a ceder, qualquer escolha que esta faça, entre o consentir ou não, apresentar-se-á sempre incompleta.

Nas situações em que o consentimento reúne informação suficiente para uma escolha consciente e racional, não acompanhamos a *infeliz ideia* de que o requisito do consentimento seja interpretado como um encargo (mais um, dirão) nas transacções comerciais. Pelo contrário. O consentimento individual, esclarecido, inequívoco, corresponde a um *quesito básico para um controlo* da aquisição legal, posse e uso da informação pessoal que o seu titular cede(rá) a terceiros[70]. As vantagens – aqui focados

pública , ou ainda para a realização do interesse legítimo de uma pessoa , desde que os interesses ou os direitos e liberdades ca pessoa em causa não prevaleçam; que, em especial, para assegurar o equilíbrio dos interesses em causa e garantir ao mesmo tempo urna concorrência real, os Estados-membros são livres de determinar as condições em que os dados pessoais podem ser utilizados e comunicados a terceiros no âmbito de actividades legítimas de gestão corrente das empresas e outros organismos; que, do mesmo modo, podem precisar as condições em que a comunicação a terceiros de dados pessoais pode ser efectuada para fins de mala directa ou de prospecção feita por uma instituição de solidariedade social ou outras associações ou fundações, por exemplo de carácter político, desde que respeitem as disposições que permitem à pessoa em causa opor-se, sem necessidade de indicar o seu fundamento ou de suportar quaisquer encargos, ao tratamento dos dados que lhe dizem respeito»

69 Atente-se no processo de aquisição e registo de um imóvel. Materializado o procedimental associado, quantos não são, imediatamente após, sujeitos a assédio intenso por parte de empresas de telecomunicações?

70 «*Considerando (38) que, para que o tratamento de dados seja leal, a pessoa em causa deve poder ter conhecimento da existência dos tratamentos e obter, no momento em que os dados lhe são pedidos, uma informação rigorosa e completa das circunstâncias dessa recolha*.». Aqui faltou ousadia ao legislador, porquanto o «*deve poder ter*» do Considerando deveria ter sido redigido enquanto «**tem de ter**». Só através

meramente numa relação comercial, pessoa/empresa -, serão tanto mais óbvias quanto a relação entre estes estiver pressuposta na confiança[71]. O consentimento (ou a sua recusa), evidentemente, só poderá ser dado pelo seu titular, uma vez na posse de toda a informação pertinente para esse efeito. Consciente das circunstâncias relevantes, impacto e consequências desse seu acto para o processamento de dados pessoais, é que o "*eu*" preclude a invocação de uma violação do seu direito fundamental à identidade informacional. Mais ainda quando o consentimento revela uma cláusula de salvaguarda do responsável pelo tratamento, afastando a *ilegitimidade* da apropriação dos dados pessoais do seu titular. Daí que o consentimento não possa ser relativizado, ou minorado[72]. Mesmo quando a *mecânica rotina do consentimento, do assine aqui-assine ali-preencha a cruz acolá,* a isso nos tente. Não negligenciamos que a DPD perpassa uma ideia de subsidiariedade à legislação nacional dos seus Estados-membros. Ainda que a matéria reclamasse uma postura mais objectiva, concretizadora e harmonizadora, a interpretação nacional mais latíssima ou mais restritiva da figura do consentimento, de um ou outro EM, acabará por ficar *desamparada* em razão do *direito comercial e direito fiscal a retalho* que cobre a União e da computação em linha que o complementa. Pior

do conhecimento *da informação rigorosa e completa das circuntâncias da recolha* é que a pessoa poderá optar por ceder, ou não, de forma consciente *partes de si* a outrem.

71 Atente-se, por exemplo, em algumas das conclusões do recente inquérito, «*Whose data is it anyway?*» elaborado pelo CIM – *The Chartered Institute of Marketing*- pré-disponibilizadas, por exemplo em formato de digesto digital em: https://cimcomms.uberflip.com/i/729663-whose-data-is-it-anyway - Último acesso Out.2016.

Com efeito, as percentagens obtidas, quer pela parte das organizações quer pela parte dos consumidores, confirmam suspeitas relativamente a más práticas e a um mau uso da informação contida e objecto de tratamento, após recolha de dados pessoais. A quebra de confiança, cliente-empresa, que estas incidências, em parte, revelam, não serve a ninguém. A pessoa – enquanto cliente – refugia-se cada vez mais, para evitar ser fustigada por assédios diversos de *marketing*, afastando-se dos mercados. Por outro lado, as empresas, pensando apenas no imediato e descurando as vantagens de uma relação de confiança, de transparência e de boa-fé com (potenciais) clientes, perdem o acesso a uma panóplia de vantagens competitivas que uma gestão legal do tratamento de dados pessoais possibilitará.

Veja-se ainda, analisado o inquérito, foi possível apurar que, por exemplo *«(...) a shocking 92% of consumers do not fully understand where and how marketers, brands and organisations use their personal information and data, and one third (31%) say they have no idea about where and how their personal data is being used(...)**More than half of all consumers (57%) say they do not trust an organisation to use their data responsibly** – the biggest issue being that their information may be passed onto others without consent (40%).*», do outro lado também foi possível constatar que »(…)*Although our report reveals data discrepancies and concerns to be worryingly prevalent across the board, **two-thirds (67%) of customers actually say they would share more personal information if organisations were more open about how they will use it.***». Disponível em: «*Consumers in the dark about their own data*», em: https://exchange.cim.co.uk/blog/consumers-in-the-dark-about-their-own-data/ . Ultimo acesso Set.2016.

72 Acompanhamos ainda SOUSA PINHEIRO a propósito de uma outra incorrecção em sede de consentimento: «*A inexistência de uma redacção sem ambiguidades, no sentido da necessidade de consentimento prévio (opt in) ou o inverso (opt out)»*. - PINHEIRO (2015), *op.cit*., p. 658.

ainda quando o *desconhecimento*[73], quer da pessoa quer das organizações, *vis a vis*, cobre de intenso nevoeiro o binário razão-finalidade.

3.3.3. EM ESPECIAL, DOS DIREITOS NA DPD

No que concerne aos direitos expressamente positivados, cumpre, em primeiro lugar, relevar o **direito à informação**. Intrincado, entendemos, no próprio consentimento, a DPD optou por, quanto à tutela deste direito, proceder a uma distinção em função do procedimento da recolha de dados. Se a mesma ocorrer na presença do seu titular, opera o Artigo 10.º; pelo contrário, na ausência do titular, releva o disposto no Artigo 11.º. O direito de informação assenta, basicamente, num direito a ser informado acerca da identidade do responsável pelo tratamento, da finalidade deste, dos eventuais destinatários, e do modo como podem ser exercidos os direitos de acesso ou rectificação, com vista à garantia de um tratamento leal. De resto, o conhecimento e o acesso a esta informação pessoal, recolhida para a realização de dado tratamento (dados pessoais), esboça, em larga medida, a fundamentalidade da própria *autodeterminação informacional* da pessoa. Desprovida da informação relevante, naquilo que lhe diz respeito, a pessoa simplesmente ignora os mecanismos de reacção de que dispõe atinentes ao tratamento e ulterior desenvolvimento, travestindo-se os seus direitos numa natureza puramente formal.

Cumpre, ainda, elucidar algumas das especificidades insítas no Artigo 11.º, *i.e.*, quanto ao tratamento de dados que não são recolhidos junto do seu titular. Os dados recolhidos de *forma indirecta* demandam o responsável pelo tratamento a prestar as mesmas informações constantes do preceito anterior, no momento do registo dos dados. O mesmo raciocínio é, compreensivelmente, aplicável aos casos em que os dados são recolhidos com uma determinada finalidade e o responsável pelo tratamento inicial pretende incutir-lhes um outro fim[74]. A utilização dos dados, operada quer por recurso mediado, quer para uma nova finalidade, constituirá um novo tratamento de dados, logo o respectivo titular

73 Ainda o inquérito conduzido pelo CIM, a que aludimos previamente.

74 *Vide*, «*Considerando (39) que por vezes se tratam dados que não foram recolhidos directamente pelo responsável junto da pessoa em causa; que, além disso, os dados podem ser legitimamente comunicados a um terceiro sem que essa comunicação estivesse prevista na altura da recolha dos dados junto da pessoa em causa; que, em todos estes casos, a pessoa em causa deve ser informada no momento do registo dos dados ou, o mais tardar, quando os dados são comunicados pela primeira vez a um terceiro*.»

dos dados terá de ser informado acerca dele(s)[75]. Reiterando a impossibilidade de direitos absolutos, também o direito de informação pode ceder[76], especialmente nos casos *do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica,* quando *a informação da pessoa em causa se revelar impossível ou implicar esforços desproporcionados ou quando a lei dispuser expressamente o registe dos dados ou a sua divulgação*[77].

Por sua vez, sem ter que invocar a finalidade, o titular dos dados pessoais tem um **direito de acesso** aos seus próprios dados, *livremente e sem restrições, com periodicidade razoável e sem demora ou custos excessivos*[78], independentemente da natureza da respectiva posse, seja pública ou privada. Previsto no artigo 12.º, o direito de acesso acaba por completar *a posição jurídica de "autodeterminação informacional" expressa no direito de informação* (PINHEIRO, 2015)[79]. Da simbiose do direito de informação com o direito de acesso, a pessoa *passa a poder controlar* as condições de recolha dos seus dados pessoais, bem como o acompanhamento das ulteriores variações dos tratamentos que lhe forem acometidos. Mantendo a lógica, o exercício deste direito de acesso permite[80] a

75 Atente-se, por exemplo, na relevância da verificação do cumprimento do artigo 10.º, número 4, da Lei de Protecção de dados - Lei n.º 67/98, *i.e.*, «*No caso de recolha de dados em redes abertas, o titular dos dados deve ser informado, salvo se disso já tiver conhecimento, de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.*».

76 *Vide,* «*Considerando (40) que, no entanto, a imposição desta obrigação não é necessária caso a pessoa em causa esteja já informada; que, além disso, não existe essa obrigação caso o registo ou a comunicação dos dados estejam expressamente previstos na lei ou caso a informação da pessoa em causa se revele impossível ou exija esforços desproporcionados, o que pode ser o caso do tratamento para fins históricos, estatísticos ou científicos; que, para este efeito, podem ser tomados em consideração o número de pessoas em causa, a antiguidade dos dados e as medidas compensatórias que podem ser tomadas;*».

77 Artigo 11.º, número 2, da DPD.

78 Artigo12.º, alínea a), da DPD.

79 SOUSA PINHEIRO, Alexandre, Op.*cit*, p.. 659.

80 *Vide*, por exemplo, a posição do Tribunal de Justiça, na *Decisão Rijkeboer* (C-553/07) de 7 de Maio de 2009. «1- *O direito ao respeito da vida privada, enunciado no artigo 1.°, n.° 1, da Directiva 95/46, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados implica que a pessoa em causa possa assegurar-se de que esses dados pessoais são tratados com exactidão e de forma lícita, ou seja, em especial, que os dados de base que lhe dizem respeito são exactos e são enviados a destinatários autorizados. Como referido no quadragésimo primeiro considerando da directiva, para poder efectuar as verificações necessárias, a pessoa em causa deve dispor de um direito de acesso aos dados que lhe dizem respeito e que estão em fase de tratamento*.

2- *O artigo 12.°, alínea a), da Directiva 95/46 determina que os Estados-Membros garantirão um direito de acesso à informação sobre os destinatários ou categorias de destinatários e sobre o conteúdo da informação comunicada não apenas relativamente ao presente mas também no que respeita ao passado. Cabe aos Estados-Membros fixar o prazo durante o qual essa informação deve ser conservada e o acesso correlativo a esta que representem um equilíbrio justo entre, por um lado, o interesse da pessoa em causa em proteger a sua vida privada, designadamente através das vias de intervenção e de recurso previstas pela Directiva 95/46, e, por outro, o ónus que a obrigação de conservar essa informação representa para o responsável pelo tratamento.*

rectificação, o apagamento ou o bloqueio dos dados pessoais inexactos, incompletos, desactualizados cujo tratamento não cumpra o disposto na presente directiva[81]. Concomitantemente, a esfera de protecção deste direito é passível de violação. Assim o prescreve, no domínio das derrogações e restrições, o artigo 13.º. Postulando as interjeições do Considerando (43)[82], o direito de acesso pode, à semelhança do direito de informação, ser restringido sempre que *imperativos de segurança do Estado, da defesa, da segurança pública, dos interesses económicos ou financeiros importantes de um Estado-membro ou da União,* entre outros, o imponham.

Por último, cumpre-nos ainda retratar o **direito de oposição**[83]. Este direito apresenta-se-nos como uma espécie de *remédio jurídico preventivo ou cautelar na disposição do titular dos dados, contra soluções típicas, a posteriori, próprias dos sistemas judiciais*[84]. Como veremos, surge como um instrumento impeditivo do esvaziamento legal do direito à *autodeterminação informacional*, precisamente naqueles casos em que a lei pretenda estabelecer critérios adicionais de legitimação do tratamento de dados pessoais, à margem da vontade ou interesse do seu titular, adoptando, *in casu*, uma natureza de *opt out*[85] (PINHEIRO, 2015). A DPD reconhece, genericamente, o direito de oposição do seu titular, *salvo disposição em contrário do direito nacional*[86]. Aqui, compelindo a uma

---

3- *Uma regulamentação que limite a conservação da informação sobre os destinatários ou categorias de destinatários e sobre o conteúdo dos dados transmitidos a um período de um ano e correlativamente limite o acesso a essa informação, quando os dados de base são conservados por muito mais tempo, não representa um equilíbrio justo entre os interesses e obrigações em causa, a não ser que se demonstre que um período de conservação dessa informação mais longo constitui um ónus excessivo para o responsável pelo tratamento. Cabe ao órgão jurisdicional nacional efectuar as verificações necessárias*.» Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62007CJ0553&from=EN . – Ùltimo acesso Set.2016.

81 Artigo 12.º, alínea b), da DPD.

82 «*Considerando (43) que restrições aos direitos de acesso e informação e a certas obrigações do responsável pelo tratamento podem igualmente ser previstas pelos Estados-membros na medida em que sejam necessárias para proteger, por exemplo, a segurança do Estado, a defesa, a segurança pública, os interesses económicos ou financeiros importantes de um Estado-membro ou da União, e para a investigação e a repressão de infracções penais ou de violações da deontologia das profissões regulamentadas; que há que enumerar, a título das excepções e restrições, as missões de controlo, de inspecção ou de regulamentação necessárias nos três últimos domínios citados referentes à segurança pública, ao interesse económio ou financeiro e à repressão penal; que esta enumeração de missões respeitante aos três domínios referidos não prejudica a legitimidade de excepções e de restrições por razões de segurança do Estado e de defesa;»*

83 Artigo 14.º, da DPD.

84 JANEIRO, Domingo Bello. "La Protección De Datos De Carácter Personal En El Derecho Comunitario" *in Anuario da Facultade de Dereito da Universidade da Coruña*, Nº 5, 2001, p.139.

85 SOUSA PINHEIRO, Alexandre, *op.cit*., p.. 660.

86 Artigo 14.º, alínea a), da DPD: «*Os Estados-membros reconhecerão à pessoa em causa o direito de: a)Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7.º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam*

oposição justificada por parte do titular, em princípio, o tratamento dos dados pessoais - lícito à luz das regras jurídicas nacionais do EM - *deixa de poder incidir sobre esses dados*. Não obstante o exposto, conferindo alguma margem de conformação interna a cada EM, a DPD converte a regulação deste direito de oposição num alvo fácil e previsível: «(…) *no está en absoluto exenta de críticas: este derecho sería realmente de gran importancia si se contemplara en el sentido lato de la palabra. En verdad se limita la efectividad de este derecho a unos cuantos supuestos muy concretos, talvez con el ánimo de mitigar el amplio margen concedido al principio del consentimiento del artículo 7 donde se utilizan expresiones muy vagas de amplio contenido*» (JANEIRO, 2001)[87].

Um último registo, sumário, a propósito do direito consagrado na alínea b) do artigo 14.º[88]. Com efeito, a terminologia usada - "*efeitos de mala directa*" - conjectura aos ficheiros mantidos com fins de publicidade e/ou de *marketing* directo. Gostaríamos de vincar a transferência de bases e/ou de listas de dados pessoais para terceiros e para utilização com esta *finalidade*. Neste conspecto, pretendemos salientar, em particular, as seguintes observações:

i) De antemão, concedemos que, perante a não existência do segmento *binário* inicial da recolha dos dados – de que já demos conta - de *razão+finalidade*, a DPD postule um direito a opor-se ao tratamento de dados por parte do seu titular. Obviamente, porque *marketing* directo não pressupõe na sua génese o consentimento prévio dos titulares dos dados, mas, tão-só, o posterior exercício do direito de oposição[89].

ii) Intrincado neste apontamento, antecipando contudo, suscita-nos a seguinte perplexidade: como garantir a efectividade de um direito de oposição perante situações em que este só pode ser exercido se os titulares dos dados tiverem conhecimento da

---

respeito sejam objecto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efectuado pelo responsável deixa de poder incidir sobre esses dados;»

87 JANEIRO, Domingo Bello, *op.cit.*, p.139.

88 «(*b)*) *Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de mala directa ; ou ser informada antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de mala directa ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações.*

Os Estados-membros tomarão as medidas necessárias para garantir que as pessoas em causa tenham conhecimento do direito referido no primeiro parágrafo da alínea b).»

89 Novamente, o Considerando (30), parte final: «(Considerando que, para ser lícito,)(…) *do mesmo modo, podem precisar as condições em que a comunicação a terceiros de dados pessoais pode ser efectuada para fins de mala directa ou de prospecção feita por uma instituição de solidariedade social ou outras associações ou fundações, por exemplo de carácter político, desde que respeitem as disposições que permitem à pessoa em causa opor-se, sem necessidade de indicar o seu fundamento ou de suportar quaisquer encargos, ao tratamento dos dados que lhe dizem respeito.*»

existência do tratamento? Ou seja, após o facto consumado do tratamento dos mesmos? No caso, cogite-se, de situações de recolha massiva de dados pessoais[90], feita através de fontes abertas como a *Internet*. Adite-se que, após o *mapeamento automatizado de perfis*[91] de pessoas singulares, os dados pessoais, *desamparados*, ficam à disposição de *decisões individuais automatizadas*[92]. Na pungente e avassaladora realidade de *big data* em que vivemos, acompanhamos as interjeições de DONEDA (2008)[93], a propósito da «*característica peculiar do dano causado pelo tratamento abusivo de dados pessoais: ele pode ser opaco, quase invisível, pois o dano em si pode-se diluir em várias manifestações sem que o prejudicado se dê conta de seu nexo específico com o tratamento de seus dados pessoais. Tome-se por exemplo uma negativa de um empréstimo bancário baseada em uma avaliação da capacidade de endividamento do solicitante que utilizou dados pessoais coletados de forma abusiva, ou que não correspondiam à realidade, sem que o solicitante sequer tenha a consciência de que tais dados falsos estavam sendo levados em conta. Ou igualmente em outras situações, como a de uma apólice de seguro-saúde de uma pessoa que pode eventualmente ser mais restritiva para ela do que para as demais*

90 A propósito da fábula dos dados pessoais, e da natureza das informações daí retiradas, de valor negligenciável - «***É apenas um mero dado, sem importância***». Esta sucumbe perante a realidade e estado da arte tecnológica presentes. Assim, FROSINI, VIttorio, *Contributi ad un diritto dell'informazione*. Napoli: Liguori, 1991, pp. 128-129. *Apud. DONEDA, op.cit.*, «(quanto à natureza das informações), *a sua necessidade e utilização. Estas dependem em parte da finalidade para a qual a coleta de dados é destinada, e de outra parte, da possibilidade* ***de elaboração e de conexão próprias da tecnologia da informação. Nesta situação, um dado que, em si, não aparenta possuir nenhuma importância, pode adquirir um novo valor****; portanto, nas atuais condições do processamento automático de dados, não existe mais um dado 'sem importância'"».*

91«(...) profiling is an everyday experience of reducing complexity. Human beings tend to categorise and generalise what happens to them in order to make reality more easily understandable. Machines can be programmed by human beings to automatically process information.(...) Automated profiling is based on "automated functions that collect and aggregate data" and develop into "automation technologies that can move beyond advice on decision-making, taking a load of low-level and even high-level decisions out of human hands". ***Autonomic profiling describes the process whereby the human role is minimized and the decision making process is entirely driven by the machine*** *(Hildebrandt, 2006, 2008a).* ***Autonomic profiling "goes one step further than automated profiling". Ambient Intelligence and Internet of Things are based on autonomic profiling. The machines drive the decision making process, providing for a readjusted environment based on their profiling and without calling for human intervention.*** *»* DEFINING PROFILING, V. Ferraris (AMAPOLA); F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva(UNICRI), and Internal reviewer: B.J. Koops. pp. 4-5. - http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf . – Último acesso Set.2016.

92 «*Artigo 15° Decisões individuais automatizadas - 1 . Os Estados-membros reconhecerão a qualquer pessoa o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento.*»

93 DONEDA, Danilo. *Privacidade, Vida Privada E Intimidade No Ordenamento Jurídico Brasileiro. Da Emergência De Uma Revisão Conceitual E Da Tutela De Dados Pessoais*. (2008) Âmbito Jurídico, Rio Grande, XI, n. 51. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460 . – Último acesso Set.2016

pelo fato da seguradora ter tido acesso às suas informações genéticas que atestam uma propensão para o desenvolvimento de uma determinada patologia, dificultando o acesso à saúde em relação às demais pessoas.».

iii) De facto, o dano, infligido ou potencial, reclama uma conclusão jurídica contundente. A "*falha original*" que secundamos, apontada por SOUSA PINHEIRO, da doutrina da «*protecção de dados pessoais*» não poderá perder mais tempo sem acentuar a tónica do debate em torno da protecção, no digital, da pessoa. O ***que está em causa não são "dados" ou a sua "protecção", mas a pessoa*** (PINHEIRO, 2015)[94].

94 SOUSA PINHEIRO, *op.cit.*, p. 827.

4. A PROTECÇÃO DE DADOS NO ORDENAMENTO JURÍDICO-CONSTITUCIONAL PORTUGUÊS

Historicamente, a Constituição da República Portuguesa, na sua versão originária de 02 de Abril de 1976[95], assumiu um dado pioneirismo internacional ao tratar da questão da protecção dos dados pessoais e ao contribuir para o aprofundamento dos direitos fundamentais. Com efeito, no seu artigo 35.º[96], a CRP (versão originária) postulava o direito de todos os cidadãos de tomar conhecimento da informação constante de registos mecanográficos a seu respeito e do fim a que se destina(va)m tais informações, conferindo-lhes o direito de exigir a rectificação dos dados e a sua actualização. Sinalizando a proibição do uso da informática para o tratamento de dados de natureza sensível, como os dados referentes a convicções políticas, fé religiosa ou vida privada, permitia, contudo, que, desconsiderados (não identificáveis) da pessoa a que dissessem respeito, pudessem ser utilizados para o tratamento de dados com fins estatísticos. Releve-se ainda – por imperativos categóricos históricos – a prescrição constitucional da *proibição da redução da pessoa a um número nacional único de cidadão*.

Por entre revisões constitucionais, até à redacção actual do artigo 35.º da CRP[97], notamos a constitucionalização da proibição *do acesso de terceiros a ficheiros com dados pessoais*

95CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA (versão originária). Disponível em: http://www.tribunalconstitucional.pt/tc/content/files/crp/crp1976.pdf . – último acesso Set.2016.

96 «*ARTIGO 35.º (Utilização da informática)*
1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
3. É proibida a atribuição de um número nacional único aos cidadãos.»

97 «*Artigo 35º -(Utilização da informática)*
1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

e a respectiva interconexão, bem como os fluxos de dados transfronteiras, salvo em casos excepcionais previstos na lei (número 2), bem como a introdução e remissão para a lei da definição *do conceito de dados pessoais para efeitos de registo informático (número 4)*[98]; a extensão da protecção a conferir aos dados pessoais que passou a *considerar bases e bancos de dados e respectivas condições de acesso, constituição e utilização por entidades públicas e privadas*, assim como a remissão para a lei[99] *do regime aplicável aos fluxos de dados transfronteiras, estabelecendo formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional (número 6)*[100]*;* até ao acompanhamento, pela necessidade, da transposição da Directiva n.º 95/46/CE, postulando a *estabilização conceptual* actual do artigo 35.º da CRP[101].

Em termos sumários, diríamos que a previsão constitucional da tutela dos direitos, no que à *utilização da informática* diz respeito, projecta-se essencialmente sobre os dados pessoais, implicando, de um lado, direitos e garantias para os titulares destes dados e, por outro, criando obrigações para quem os trate: seja na recolha, transmissão, cedência, conservação, qualidade e segurança da informação, bem como quanto às condições em que esta possa ser usada. A previsão de vários direitos, tais como o direito de acesso, o direito de rectificação e actualização, o direito a conhecer a finalidade, entre outros, respaldam a protecção do tratamento de dados pessoais sob supervisão da entidade administrativa independente competente para o efeito, *in casu*, a CNPD (a que regressaremos mais à frente).

4.1. EM ESPECIAL, O ÂMBITO PROTECTIVO DO DIREITO À IDENTIDADE INFORMACIONAL

A temática dos dados pessoais e do tratamento de dados pessoais, no contexto jurídico-constitucional, encontra amparo no valor fundamental da *autodeterminação informacional*. *A estrutura garantística de carácter procedimental que cumpre à*

7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.»
98 Revisão constitucional de 1982, Lei n.º 1/82, de 30/09.
99 Que finalmente viria a operacionalizar o Artigo 35.º da CRP, por via da Lei n.º 10/91, de 29/04 - Lei da Protecção de Dados Pessoais face à Informática.
100 Revisão constitucional de 1989, Lei n.º 1/89, de 08/07.
101 Revisão constitucional de 1997, Lei n.º 1/97, de 20/09.

protecção de dados, permite autonomiza-la como uma forma de concretização da "autodeterminação informacional", i.e., se a protecção de dados é pensada como uma garantia, ex ante o seu fundamento - a autodeterminação informacional - exprime-se como uma liberdade[102]. Daqui decorre a necessidade de conferir protecção jurídica a "todos" os elementos de informação pessoal. Em virtude dos avanços tecnológicos e das técnicas, numa afirmação presente de *big data*, urge mitigar a possibilidade de esta formar um "*todo subjectivo*"[103], uma vez coligida informação esparsa[104].

Efectivamente, arrancando da dignidade da pessoa humana para o ordenamento jurídico-constitucional português[105], a construção dogmática do direito à identidade informacional deverá encerrar a construção de um direito de defesa da pessoa[106], de um direito de controlo dos seus dados pessoais[107], que lhe permita superintender a disponibilização *online* destes, independentemente de ter sido anteriormente autorizada, ou não, pelo próprio[108].

---

102 SOUSA PINHEIRO, Alexandre, *Op.cit.*, p. 805.

103 FARIA, Maria Paula Ribeiro de (2010), *in Constituição Portuguesa Anotada, coord. Jorge Miranda e Rui Medeiros,* Anotação ao artigo 35.º; Coimbra Editora; p. 788.

104 «*In the case of big data, (personal) data are used* ***to extract non-trivial new information out of the given data via the technique of (predictive) data mining****. The big data entrepreneurs then appropriate the (fruits of) the newly discovered insights.* ***It is the "gold" that is so emphasized by commentators.***». SAX, Marijn, "BIG DATA: Finders Keepers, Losers Weepers'?" *in Ethics and Information Technology, Volume 18,* March 2916, Issue 1, p. 28.

105 Conforme o pensamento de OTERO: «*o homem é digno porque é pessoa. A dignidade não lhe é atribuída de fora, não é um a mais, é intrinsecamente decorrente da própria característica de ser pessoa, que é dialecticamente unitária desde a concepção até à morte. O homem é pois digno porque é dele constitutivo um projecto a realizar.*». Sobre este princípio – OTERO, Paulo (2007*) Instituições Políticas e Constitucionais, Volume I,* Almedina: Coimbra; pp. 545 e segs;

106 Atentemos, por exemplo, nas declarações da Comissária responsável pela Justiça e Vice-Presidente da Comissão, Viviane Reding, na altura: *«A proteção dos dados pessoais é um direito fundamental de todos os europeus, mas os cidadãos nem sempre sentem que controlam plenamente os dados que lhes dizem respeito. As nossas propostas contribuirão para criar um clima de confiança nos serviços em linha porque as pessoas estarão melhor informadas sobre os seus direitos e controlarão melhor as informações que lhes dizem respeito. A presente reforma cumprirá esse objetivo, simplificando a vida das empresas e reduzindo as suas despesas. Um quadro jurídico sólido, claro e uniforme a nível da UE contribuirá para libertar o potencial do mercado único digital e promover o crescimento económico, a inovação e a criação de emprego».* Disponível em: http://europa.eu/rapid/press-release_IP-12-46_pt.htm . – Último acesso Set.2016.

107 «(…)*O enunciado linguístico* dados *é o plural da expressão latina* datum *e está utilizada na Constituição no sentido que hoje lhe empresta a ciência informática: representação convencional de informação sob a forma analógica ou digital possibilitadora do seu tratamento automático (introdução, organização, gestão e processamento de dados).(...)O desenvolvimento dos meios tecnológicos e o crescente recurso a meios electrónicos que deixam "*pegadas electrónicas*"(...) tornam cada vez mais importantes as garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados.*». CANOTILHO, Gomes/ MOREIRA/Vital. Constituição Da República Portuguesa Anotada, (2007) Volume I, 4.ª Edição, Coimbra Editora, p. 550.

108 Alguma doutrina sustenta que está em causa a tutela da reserva sobre factos cujo reconhecimento por terceiros deve depender de decisão do seu titular, independentemente de respeitarem ao núcleo mais estrito da sua vida privada ou de serem inóquos – FARIA, Maria Paula Ribeiro de (2010), *in Constituição*

Nesta perspectiva, estaremos na presença de um direito de defesa do controlo da rastreabilidade dos dados pessoais pelo seu titular, no controlo da sua pegada digital e do inerente direito à reserva da vida privada, um verdadeiro e moderno[109] *direito à sua identidade informacional*[110], radicado na *dignidade da pessoa humana, no desenvolvimento da personalidade, na integridade pessoal e na autodeterminação informativa* (CANOTILHO, 2007). Desde logo, do princípio da dignidade da pessoa humana colhe a protecção da "*Fórmula do Objecto",* perante actuações estatais, para impedir que a pessoa *seja degradada ao nível de uma coisa ou de um objecto no actuar estatal,* precludindo eventuais *afectações desnecessárias, fúteis ou desproporcionais,* como sejam aquelas que não sejam justificadas pela estrita necessidade de realização de fins, valores ou interesses dignos de protecção jurídica e efectuadas de acordo com a Constituição[111]. Em conformidade, toda e qualquer actuação estatal que fira *uma pretensão jurídico-constitucionalmente protegida de os cidadãos não terem a sua liberdade individual negativamente afetada a não ser quando tal seja estrita e impreterivelmente exigido pela prossecução, por parte dos poderes públicos, de outros valores igualmente dignos de proteção jurídica*[112]*,* encontrar-se-á irremediavelmente inquinada, por preterição de requisitos materiais de conformidade com a Constituição. Trata-se de dar a cada um, através de um complexo feixe de direitos, o direito de controlar a informação disponível a seu respeito, obstando a que a pessoa se torne «*simples objecto de informações*, *(...)quanto mais os dados relacionam a dignidade, a personalidade e a autodeterminação das pessoas, tanto mais se impõem restrições quanto à sua utilização e recolha(...).»*[113]. Integra aquele conjunto de direitos cujo conteúdo tem uma maior proximidade do que outros no que se refere a uma "*imposição moral, política e jurídica*

Portuguesa Anotada, coord. Jorge Miranda e Rui Medeiros, Anotação ao artigo 35.º; Coimbra Editora; p. 789.

109 CANOTILHO, Gomes/MOREIRA/Vital (2007*) op.cit.,* p. 551.

110 «*A designação do direito à identidade informacional absorve o conteúdo do direito à protecção de dados, eliminando as insuficiências da referida fórmula, desde sempre considerada inadequada. O novo direito, para além de tratar matéria inovadora, introduz terminologia rigorosa dotada de clareza semântica.*» PINHEIRO, Alexandre Sousa, *op.cit.,* p. 829.

111 NOVAIS, Jorge Reis (2004) *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra Editora: Coimbra, p. 57.

112 *Ibidem, idem.*

113 CANOTILHO, Gomes/MOREIRA/Vital (2007*) op.cit.,* p. 551.

de respeito e protecção"[114], atenta a sua inserção nos direitos de personalidade, sem os quais, não há Estado de Direito democrático.

Acresce uma dimensão positiva, que integra faculdades e poderes de natureza positiva, expressamente positivados no ordenamento jurídico-constitucional português. Nos termos do artigo 35.º, da Constituição da República portuguesa, é reconhecido não apenas o direito de acesso aos dados e registos informáticos que lhes digam respeito, como também o direito de rectificação e cancelamento dos dados, o direito ao sigilo sobre eles, bem como o direito ao respectivo não tratamento[115]. Cumpre ainda destacar, entre as prestações positivas adjacentes a esta posição jurídica de vantagem, o direito a uma prestação normativa por parte do Estado, pressuposto do exercício da sua dimensão de liberdade. Efectivamente, a doutrina sustenta a vinculação do Estado na adopção de medidas normativas com vista à eficácia plena da autodeterminação da pessoa perante o uso da informática[116].

114 MORAIS, Carlos Blanco (2014), *Curso de Direito Constitucional, Tomo II*, Coimbra Editora; pp. 465 e segs e, em especial, p. 469.

115 FARIA, Maria Paula Ribeiro de (2010), *in Constituição Portuguesa Anotada, coord. Jorge Miranda e Rui Medeiros,* Anotação ao artigo 35.º; Coimbra Editora; p. 789.

116 A propósito dos direitos fundamentais em matéria de defesa contra o tratamento informatizado de dados pessoais, fala-se mesmo num *Habeas Data* ao constituírem garantia de uma liberdade de natureza fundamental dos tempos modernos. – FARIA, Maria Paula Ribeiro de (2010), *in Constituição Portuguesa Anotada, coord. Jorge Miranda e Rui Medeiros,* Anotação ao artigo 35.º; Coimbra Editora; p. 789.
Note-se, porém, que, tal como todos os outros direitos e liberdades, estão sujeitos a ponderações com os bens constitucionalmente protegidos, nos termos do artigo 18.º, n.º 2, segunda parte - (segredo de Estado, segurança interna, segredo de justiça). Ainda sobre *habeas data,* veja-se a propósito a doutrina argentina sobre a matéria, por exemplo, sobre o qual, nos termos do art.º 43 da Constituição Argentina, *«(...) que recepta el amparo genérico, el amparo colectivo, el habeas data y el habeas corpus (...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidade, que consiste en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No poderá afectarse el derecho de información periodística.*», Oteiza,Eduardo em «*Información privada y habeas data*», p. 170, disponível em: http://www.palermo.edu/derecho/publicaciones/pdfs/revista_juridica/Especiales_SELA/SELA%201998%20-%20Ed%201999/04SELA98Juridica13.pdf

4.2. A LEI DE PROTECÇÃO DE DADOS PESSOAIS [117] NA SENDA DO DIREITO EUROPEU

Transpondo e recebendo na ordem jurídica nacional o regime jurídico europeu derivado da Directiva 95/46/CE[118], o legislador nacional procedeu à fundação da *autoridade de controlo nacional,* internamente, enquanto entidade administrativa independente, com poderes de autoridade, competente para a tutela da temática dos dados pessoais e da sua protecção – a Comissão Nacional de Protecção de Dados[119]. Em acréscimo, passou a prever a possibilidade de promoção de um regime de *compliance*[120]; bem como efectivou regimes, sancionatório[121] e criminal, específicos[122]. Em termos genéricos e substanciais, o legislador nacional *não inovou* muito quanto ao regime propugnado na DPD.

4.2.1. FISCALIZAÇÃO ADMINISTRATIVA INDEPENDENTE E NOTAS GENÉRICAS SOBRE O REGIME MATERIAL DA LPDP

4.2.1.1. No que concerne à *autoridade nacional* de protecção de dados, a CNPD *é a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei*[123]. O respetivo elenco de poderes e competências encontra-se descrito ao longo dos artigos 22.º e seguintes, entre os quais os de " (…) *a) investigação e de inquérito, podendo aceder aos dados objecto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo; b) de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem*

117 Lei n.º 67/98, de 26 de Outubro - LEI DA PROTECÇÃO DE DADOS PESSOAIS – (LPDP) (*transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados*). Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=156&tabela=leis. - Ultimo acesso Set.2016

118 *Vide* artigos 2.º e seguintes, da LPDP.

119 A Comissão Nacional de Protecção de Dados, que sucedeu à Comissão Nacional de Protecção de Dados Informatizados, *é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República.* – Artigo 21, n.º1, da LPDP.

120 *Vide* Artigo 23.º, número 1, alínea O), conjugado com o artigo 32.º da LPDP.

121 *Vide* Artigo 35.º e seguintes, LPDP.

122 *Vide* Artigo 43.º e seguintes, da LPDP. Note-se que, fruto da exponenciação que o tratamento de dados operado pela realidade de *big data* e dos potenciais danos que tal acarreta para a tutela jurídica efectiva da pessoa singular, em 2015, por força da **Lei n.º 103/2015, de 24 de Agosto**, foi aditado um novo crime à lista original da LPDP, que passou a criminalizar as condutas de *quem insira ou facilite a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para outrem ou para causar prejuízo,* punindo-as *com pena de prisão até 2 anos ou com pena de multa até 240 dias* e agravando-as *para o dobro se dessa conduta resultar efetivo prejuízo para uma pessoa*. **Artigo 45-A - Inserção de dados falsos**, números 1 e 2, da LPDP.

123 Artigo 22.º, n.º1, da LPDP.

como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território português; c) de emitir pareceres prévios ao tratamento de dados pessoais, assegurando a sua publicitação[124]. Realce-se uma nota particular para um poder (não exclusivo) da CNPD, como seja o de, em caso de incumprimento reiterado pelo responsável pelo tratamento *das disposições legais em matéria de dados pessoais,* poder *advertir ou censurar publicamente o responsável pelo tratamento*[125].

Por sua vez, do lado das competências, destacaríamos, em particular, a competência *para (i) autorizar excepcionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 5*[126]*; (ii) Fazer assegurar o direito de acesso à informação, bem como do exercício do direito de rectificação e actualização*[127]*; (iii) Efectuar, a pedido de qualquer pessoa, a verificação de licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação*[128]*; (iv) Apreciar as reclamações, queixas ou petições dos particulares*[129] *; (v) Emitir parecer sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais*[130]. Obviamente*, no exercício das suas funções, a CNPD profere decisões com força obrigatória, passíveis de reclamação e de recurso para o Tribunal Central Administrativo*[131]. Resulta, desta forma claro, que a CNPD, integrada na administração independente do estado, e portanto atópica quer à sua administração pública directa quer indirecta, corresponde a um órgão administrativo do estado com poderes e competências de tipo *quase-jurisdicional*, vinculada nos termos da Constituição[132] e da lei[133], ao respeito pelos "*preceitos constitucionais respeitantes aos direitos, liberdades e garantias"*.

124 Artigo 22.º, n.º3, da LPDP.
125 Artigo 22.º, n.º4, da LPDP.
126 Artigo 23.º, n.º1, alínea c), da LPDP.
127 Artigo 23.º, n.º1, alínea g), da LPDP.
128 Artigo 23.º, n.º1, alínea j), da LPDP.
129 Artigo 23.º, n.º1, alínea k), da LPDP.
130 Artigo 23.º, n.º1, alínea a), da LPDP.
131 Artigo 23.º, n.º3, da LPDP.
132 *Ex vi* Artigo 18.º, n.º1 da CRP.
133 *Ex vi* Artigo 22.º, n.º1, da LPDP.

A LPDP aplica-se ao tratamento de dados pessoais informatizados ou manuais[134]. Por um lado, tutela a temática em torno do tratamento de dados pessoais efectuado: *a) No âmbito das actividades de estabelecimento do responsável do tratamento situado em território português; b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional; c) Por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia*[135]. Por outro lado, aplica-se ainda, *à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português*[136].

4.2.1.2. No confronto com a directiva europeia, cabe reiterar o nosso comentário, porquanto, em traços gerais, a LPDP não deriva muito do regime jurídico europeu que transpôs. Com efeito, tendo sido este já analisado, previamente, em substância, notamos apenas que *o legislador nacional revelou uma pura opção material*[137], própria, na transposição, na matéria específica atinente ao direito de acesso em circunstâncias envolvendo situações de segurança do Estado e prevenção ou investigação criminal[138]. Ademais, o articulado da LPDP, divergindo somente na numeração, insiste, como regra, que o titular dos dados pessoais seja conhecedor da natureza do tratamento, das respectivas finalidades, de quem pode nele intervir, do modo como pode vir a exercer os seus direitos de acesso, informação, oposição, rectificação ou correcção, entre outros. Nota-se, por exemplo, a insistência na fundamentalidade da relação do binómio *direito à informação–direito de acesso*, constituindo-os como dois elementos fulcrais de todo o direito de protecção de dados. O primeiro precedendo o segundo, notamos que:

i) A lei revigora o cumprimento das disposições relativas ao dever de informar, nos casos em que a recolha decorra directamente do seu titular, e este pretende obter as informações relativas: «*a) Identidade do responsável pelo tratamento e, se for caso disso, do seu representante; b) Finalidades do tratamento; c) Outras informações, tais*

134 Artigo 4.º, n.º1, da LPDP.
135 Artigo 4.º, n.º3, da LPDP.
136 Artigo 4.º n.º 4, da LPDP.
137 SOUSA PINHEIRO, *op.cit.*, p.. 727
138 Concretamente, os artigos 8.º a 11.º, números 2 a 4.

como: (i) Os destinatários ou categorias de destinatários dos dados; (ii) O carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder; (iii)A existência e as condições do direito de acesso e de rectificação, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir ao seu titular um tratamento leal dos mesmos.[139]»;

ii) A lei exclui apenas o dever de informar nos casos em que o titular já tivesse tido conhecimento das informações a prestar[140]; que o tratamento dos dados seja *efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária*[141]; ou *mediante disposição legal ou deliberação da CNPD, por motivos de segurança do Estado e prevenção ou investigação criminal, e, bem assim, quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação do titular dos dados se revelar impossível ou implicar esforços desproporcionados ou ainda quando a lei determinar expressamente o registo dos dados ou a sua divulgação*[142].

iii) Quanto ao direito de acesso, o argumentário expendido a propósito da DPD, é válido em moldes análogos.

4.2.2. ALGUNS *DADOS SENSÍVEIS* NA DOUTRINA DA CNPD: EM ESPECIAL, OS PARECERES N.º 28/2016 E 36/2016

Na temática dos dados pessoais, optamos por vincar, somente agora, quanto à qualidade de alguns dos dados pessoais, os, assim denominados, *dados sensíveis*. Justamente após termos caracterizado a competência própria da CNPD para a emissão de pareceres sobre disposições legais, bem como termos salientado o poder de defesa dos direitos, liberdades e garantias que lhe compete, enquanto *guardiã* da Constituição. Trazemos para discussão dois pareceres, máxime pela proximidade temporal com que foram proferidos, quanto à apreciação de projectos de lei em curso. Escolhemos estes, em especial, dado o grau de acutilância (*a tentativa*) de afectação desvantajosa dos direitos, liberdades e garantias implicados.

139 Artigo 10.º, n.º1, da LPDP.
140 Artigo 10.º, n.º 1, da LPDP.
141 Artigo 10.º, n.º 6, da LPDP.
142 Artigo 10.º, n.º 5, da LPDP.

Os tratamentos de perfil relacionados com matérias de saúde são autonomizados como dados sensíveis. Com efeito, para efeitos da *utilização da informática*, a tipicidade de dados sensíveis na CRP não é fechada. Pelo contrário. Atente-se, por exemplo, na jurisprudência do Tribunal Constitucional (doravante, TC), que no seu Acórdão n.º 355/97, o Tribunal considerou, apesar da sua *ausência* (literal) do art.º 35.º da CRP, que *os dados de saúde integram a categoria de dados relativos à vida privada, tais como as informações referentes à origem étnica, à vida familiar, à vida sexual, condenações em processo criminal, situação patrimonial e financeira(...), fazem parte da vida privada de cada um.(...)desse modo se impedindo sobre eles qualquer tratamento informatizado*[143]. Por conseguinte, o TC procedeu à sua integração nos dados *originários* de vida privada[144], inviabilizando que o legislador ordinário *sobre eles se pronuncie por via que não seja a de lei da Assembleia da República ou de decreto-lei por esta autorizado* (…), ferindo de inconstitucionalidade, por violação da reserva de lei restritiva, qualquer tentativa legislativa que não observe a exaustividade dos respectivos requisitos constitucionais[145].

Em sede de dados de saúde, sensíveis por natureza, pensamos detalhadamente nas situações em que, apresentando-se, por vezes, de relativa bonomia nos seus propósitos, o legislador pretende *torcer* um pouco mais a efectividade dos direitos, liberdades e garantias. Neste conspecto, consideremos, a título de exemplo, dois pareceres emitidos, recentemente, pela autoridade nacional portuguesa competente de protecção de dados, pela CNPD. O primeiro incidiu sobre a proposta de lei que pretende criar e regular um registo oncológico nacional (RON) - o Parecer n.º 28/2016[146]; o segundo foi deliberado a propósito da proposta de lei que pretende estabelecer o regime jurídico da realização de testes, de exames médicos e de outros meios apropriados aos trabalhadores do Corpo da Guarda Prisional, com vista à detecção do consumo excessivo de bebidas alcoólicas, consumo de estupefacientes, de substâncias psicotrópicas e produtos análogos - o Parecer n.º 36/2016[147]. Ambas as iniciativas legislativas, sobre as quais a CNPD se pronuncia,

143 Acórdão n.º 355/97, de 07 de Maio de 1997, disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19970355.html . – Último acesso Set.2016.
144 *Idem*. «*(...) considera-se que o tratamento automatizado de dados relativos a doenças oncológicas integra-se na esfera de privacidade dos doentes, interferindo, nessa medida, na definição do conteúdo de vida privada, matéria respeitante a direitos, liberdades e garantias.»*
145 Desde logo o, então, Artigo 168.º, número 1, alínea b), da CRP, na versão que resultou da revisão constitucional de1989 - (actual Artigo 165.º, n.º1, alínea b),CRP).
146 Disponível em: https://www.cnpd.pt/bin/decisoes/Par/40_28_2016.pdf . – Último acesso Out.2016.
147 Disponível em: https://www.cnpd.pt/bin/decisoes/Par/40_36_2016.pdf . – Último acesso Out.2016.

mereceram escrutínio aturado, pelo grau de intrusividade e potencial lesão que representam.

4.2.2.1. No primeiro caso, parece-nos assertivo o entendimento[148] que considera que a concretização do intuito do legislador representa, além de um risco elevado de exposição da privacidade de actuais (ou passados) doentes e familiares, pela natureza da informação que congrega, ainda riscos elevados de discriminações futuras, efectivas ou potenciais. Extrapoladas pela centralização da informação e perigos de ordem variada daí decorrentes, em termos teóricos, o grau de intrusividade – sublinhe-se, tanto mais que esta informação detalhada contém um valor económico elevado, logo apetecível para os mais diversos grupos económicos – operada quer pela lei quer por quem a ela conseguir aceder *de facto*, excede(ria) largamente a margem protectiva dos direitos fundamentais das pessoas titulares desses mesmos dados. Mesmo que a vontade política seja a de passar a gestão do RON para a esfera do IPO e que o registo já devesse estar criado[149], afigura-se-nos de difícil concretização a sobredita legislação. Pelo menos, tal como foi apresentada. A eficiência e o utilitarismo (tão em voga) da medida não poderão ser usados como pressupostos qualitativos para aferir da necessidade de efectivar mais uma torção nos direitos, liberdades e garantias.

Por conseguinte, o legislador antes de se propôr nestes termos em que apresentou, cabe-lhe responder às questões rogadas no parecer *sub judicio*, que reclama a elaboração prévia de um *estudo do impacto nos direitos fundamentais de uma tal opção política, do qual tivessem sido retiradas conclusões claras quanto à ponderação dos valores fundamentais em causa e tivessem resultado soluções, sobretudo tecnológicas, que, sem afectar a finalidade deste registo, salvaguardasse, ao menos, a identidade dos doentes oncológicos*.

4.2.2.2. Por sua vez, quanto ao Parecer n.º36/2016, nova e naturalmente, sufragamos o entendimento expendido pela sua relatora. A regulação, mesmo que operada por lei, de dados pessoais de natureza sensível, encontra-se sujeita a um regime reforçado de

148 Acompanhamos, liminarmente, a apreciação desenvolvida pela sua relatora.
149 Por exemplo, veja-se a notícia em: http://expresso.sapo.pt/revista-de-imprensa/2016-08-18-Protecao-de-Dados-chumba-registo-nacional-de-doentes-com-cancro. – Último acesso Out.2016.

protecção jurídica[150]. Ora, a proposta de lei apresenta-se (outra vez, pois a CNPD já se tinha pronunciado, quanto a esta questão em particular, previamente) *inquinada*, por preterição de requisitos materiais de constitucionalidade. Com efeito, indiciam um atropelo à tutela do tratamento de dados de natureza sensível - pois que envolvem dados de saúde e, consequentemente, de natureza reservada e privada –, apresentando-se o seu uso e tratamento, nos termos configurados pelo legislador, apenas como uma forma de controlo do comportamento dos titulares dos dados visados, o que parece resultar evidente em tal proposta. Note-se: i) a facilidade e o imediatismo da obtenção do resultado de um teste de controlo de alcoolémia, num aparelho quantitativo vulgarmente ao serviço das forças de segurança; ii) o teste/exame pode(ria) ser ordenado por um qualquer superior hierárquico.

O cenário agrava-se porquanto a entidade ou quem ela ordenar se mostra competente para a realização desses mesmos testes/exames, não sendo exigível a sua realização por um profissional de saúde ou equivalente, com especial preparação para tal. Piora mais ainda, e finalmente, porque qualquer informação daí resultante pode(ria) estar fácil e detalhadamente acessível a qualquer uma dessas entidades *supra*. Uma forma *dinâmica*, *eficiente*, de controlo laboral? E as pessoas? *Comprime-se* a sua dignidade humana a ponto tal de se *reduzirem* a um mero critério valorativo de *excel em nome de uma eficiência disciplinar*?

Ora, ante tal projecto, constatando-se que este comprime manifesta, excessiva e desnecessariamente *os direitos fundamentais à reserva da vida privada e à protecção dos dados pessoais, em violação do n.º2 do artigo 18.º da CRP e da alínea c) do n.º1 do artigo 5.º da LPDP,* acompanhamos as conclusões do aludido Parecer, as quais postulam a *reformulação da proposta de lei no sentido de passar a consagrar a obrigatoriedade da realização dos exames e testes referidos serem sempre efectuados pelos serviços de medicina no trabalho, por médicos ou profissionais de saúde*, bem como, *a informação a comunicar quanto ao resultado dos exames e testes à entidade que os solicitou apenas contenha a menção das fichas de aptidão, apto/inapto*. Naturalmente.

150 No nosso caso, por força do artigo 165.º, n.º1, alínea b) da CRP, e da conjugação dos artigos 35.º, número 3, da CRP e artigo 7.º, número 2, da LPDP.

4.3. - ALGUMAS PERPLEXIDADES DA L.A.D.A DE 2007 E DA C.A.D.A

A **Lei n.º 46/2007 de 24 de Agosto** (Lei de Acesso aos Documentos Administrativos, ou **L.A.D.A.**) – entretanto *oportuna*, e finalmente, revogada - que regula(va) o acesso aos documentos administrativos e a sua reutilização[151], bem como a respetiva interpretação da **Comissão de Acesso aos Documentos Administrativos** (doravante, **C.A.D.A**), marcaram, indelevelmente, um período sombrio de facilidade de acesso a documentos "*administrativos*", a coberto e em nome de um, suposto, generoso princípio da Administração pública aberta (com consagração constitucional, mormente no Artigo 268.º, n.º2 da CRP) ou "*transparência da Administração Pública*".

Com efeito, como veremos, a interpretação veiculada pela C.A.D.A, até muito recentemente, adoptara uma conformação interpretativa que extravasou, largamente, o objecto da relação primacial que lhe cumpria salvaguardar, *i.e.*, uma relação de transparência da Administração Pública com os particulares e/ou organizações, e não o inverso. Concedendo-se o acesso indiscriminado e sem necessidade de qualquer justificação a documentos *"administrativos", contendo partes significativas de dados pessoais totalmente desprovidos de qualquer interesse público,* a conjugação - da deficiente redacção legal - e interpretação do Artigo 3.º[152] com o Artigo 5.º[153] e excepções previstas no Artigo 6.º[154], da Lei n.º 46/2007 de 24 de Agosto, permitiu, por largos anos, uma *latência*, preocupante, de violações do direito a uma identidade informacional da pessoa singular que cumpre efectivar, revelando, ainda, uma perigosa vitracidade dos administrados ante outros semelhantes.

---

151 Tanspôs para a ordem jurídica nacional a Directiva n.º 2003/98/CE, do Parlamento e do Conselho, de 17 de Novembro, relativa à reutilização de informações do sector público.

152*«**Artigo 3.º** – **Definições:** 1 - Para efeitos da presente lei, considera-se:*
*a) «**Documento administrativo**» qualquer suporte de informação sob forma escrita, visual, sonora, electrónica ou outra forma material, na posse dos órgãos e entidades referidos no artigo seguinte, ou detidos em seu nome;*
*b) «**Documento nominativo**» o documento administrativo que contenha, acerca de pessoa singular, identificada ou identificável, apreciação ou juízo de valor, ou informação abrangida pela reserva da intimidade da vida privada.»*

153*«**Artigo 5.º - Direito de acesso**: **Todos, sem necessidade de enunciar qualquer interesse,** têm direito de acesso aos documentos administrativos, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo.»*

154 Artigo 6.º, **Restrições ao direito de acesso.**

Notando, todavia, a superação de uma *institucionalizada prática* de uma administração pública opaca, fechada, encerrada num inaudito casulo, que vigorou, não obstante, a radicalização de posições sufragadas pela C.A.D.A, desde a entrada em vigor da **Lei n.º 46/2007 de 24 de Agosto**, acabou por pôr em evidência uma série de inconstitucionalidades geradas por esta lei e *aprofundadas* pela entidade administrativa *competente*. Desde logo, o acesso a documentos da Administração, por parte de terceiros, *desinteressados*, sem a invocação de uma dada finalidade e sem a demonstração de um interesse legítimo e directo, sindica uma clara inconstitucionalidade por violação ao disposto no artigo 35.º, n.º1, da CRP, cujo conteúdo consagra o princípio da finalidade. Concomitantemente, pela frequência com que a *práxis* foi demonstrando que os administrados pretendiam ter acesso aos dados em posse da administração, não para aquilatar do correcto procedimento administrativo - que deveria suceder; não para conhecer os métodos e critérios das decisões administrativas – que poderia suceder; mas tão-só para aceder a informação administrativa para finalidades *diversas,* não declaráveis, nem justificáveis, com as quais esta *frequência e facilitismo de permissão* ao seu acesso pactuava. Mesmo coartando de forma inequívoca, desproporcional e excessiva elementares direitos e liberdades fundamentais, ínsitos no artigo 26.º, n.º1, da CRP; mesmo colidindo, irremediavelmente ainda, com a proibição de acesso a dados pessoais de terceiros contida no artigo 35.º, n.º4, da CRP.

Despudoradamente, objectivando, quando num dado momento inicial, a indicação de certos dados pessoais - como a indicação de uma morada fiscal, bem como, por exemplo, de um número de telemóvel ou telefone pessoal, entre outros - sobressai de uma indicação por parte do seu titular com a qual o princípio da finalidade se assume como exclusivo elemento constitutivo, parece-nos que, uma vez este esgotado, seria curial que a Administração pública assumisse uma posição - que lhe cumpre - de salvaguarda do direito à identidade informacional do titular dos dados, restringindo o acesso a todos os dados pessoais que não consubstanciem *procedimentos de emissão de atos e regulamentos administrativos; procedimentos de contratação pública, incluindo os contratos celebrados; gestão orçamental e financeira dos órgãos e entidades; gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações*

jurídicas[155], por parte de terceiros. Ademais, como constataremos, tal não precludiria o princípio da administração pública aberta.

4.3.1 - A L.A.D.A de 2007 e a L.A.D.A de 2016 VS a L.P.D.P.

Sem querermos aprofundar, ao detalhe, as especificidades de cada uma das versões legislativas do acesso aos documentos administrativos em causa, e na esteira de um princípio de objectivação dos motivos desta dissertação, cumpre-nos relevar alguns aspectos mais *sufragáveis* em matéria de protecção dos dados pessoais das pessoas singulares, o que, resumindo, nos colocará ante o confronto da L.P.D.P. e da L.A.D.A. (nas suas duas versões).

Assim, desde logo, mesmo que nos pareça óbvia a constatação da *nuance* fundamental no confronto entre a L.P.D.P. e a L.A.D.A, cumpre-nos destacar que o que está em causa, neste preciso confronto, é, no primeiro caso, o acesso à informação do titular dos dados, ao passo que, na L.A.D.A., o que sobressai é o acesso à informação sobre *terceiros*. Neste conspecto, propomo-nos a analisar, sucintamente, dois pareceres - os Pareceres n.º 113/2015 e 36/2016 - emitidos pela C.A.D.A, à data da vigência da (anterior) L.A.D.A, e a posição interpretativa (diametralmente oposta a estes pareceres) mais recente desta Comissão, ao abrigo da **Lei n.º 26/2016, de 22 de Agosto**[156], no caso o Parecer n.º 425/2016.

4.3.1.1 – OS PARECERES N.º 113/2015[157] E 36/2016[158] DA C.A.D.A

A) – O Parecer n.º 113/2015

No Parecer n.º 113/2015, a pleito apresentaram-se uma jornalista e a entidade requerida, a Guarda Nacional Republicana. Por esta última não ter facultado o acesso à jornalista aos: *"a) Documento(s) que contenha(m) dados em bruto sobre o valor que cada militar*

155 Artigo 3.º, n.º1, al. a), da Lei n.º 26/2016, de 22 de Agosto.
156 A Lei n.º 26/2016, de 22 de Agosto, aprovou o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro, e que, nos termos do seu Artigo 47.º, alínea b), procedeu à revogação da Lei n.º 46/2007, de 24 de agosto.
157 Disponível para consulta em: http://www.cada.pt/uploads/Pareceres/2015/113.pdf . - último acesso Nov.2016.
158 Disponível para consulta em: http://www.cada.pt/uploads/Pareceres/2016/036.pdf . - último acesso Nov.2016.

afeto ao Destacamento de Trânsito de Carcavelos recebeu, em gratificados, no ano de 2014"; b) "Documento(s) que contenha(m) o curriculum vitae do Comandante do Destacamento de Trânsito de Carcavelos B ou, na ausência deste, a listagem, em bruto, dos serviços, condecorações, cursos e demais informações sobre a visada que constem do seu processo da GNR", a queixosa formalizou a sua discordância junto da C.A.D.A.

Neste Parecer, assumindo-se formal e materialmente competente para analisar a procedência da queixa, se por um lado alinhamos com o argumentário expendido a propósito da facultação do acesso à informação relativa a vencimentos auferidos e aos "*gratificados*" - ainda que naturalmente expurgados do conhecimento de prestações numerárias relativas a prestação de alimentos e tribunais, entre outras; bem como de dados pessoais; matérias naturalmente *abrangidas pela reserva da intimidade da vida privada ou por regime especial em matéria de acesso a documentação*[159], tal não podemos conceder no tocante a um acesso livre, irrestrito, independente de justificação da finalidade, relativo à informação constante no *curriculum vitae,* e que encerrava o segundo (2.º) pedido formulado pela requerente.

Aliás, ressalta, no imediato, aquilo que nos parece ser um entendimento *bipolar:* o considerando da Comissão, no seu ponto 12, de que «" (...) *Embora a CADA entenda que, por norma, os números de telefone e de telemóvel constituem informação não nominativa, considera que já assim não será quando se esteja perante números confidenciais ou quando alguém manifeste a sua vontade de manter os mesmos sob sigilo.*"». De facto, como pode a C.A.D.A. conceder o acesso à informação contida no *CV*, se, de antemão, não sabe se o titular do telemóvel (ou telefone) manifestara a sua vontade em manter o número sob sigilo? Parece-nos, ademais, uma *abusiva interpretação*[160], atenta a inversão

159 Pontos 10 e 11 do sobredito Parecer.

160 Possivelmente apimentada pelo acolhimento nacional de alguma doutrina e jurisprudências expendidas do outro lado do Atlântico, pressupostas na ***third-party doctrine***.
Com efeito, a doutrina que vingou no caso SMITH V. MARYLAND 442 U.S. 735 (1979), sobre a qual uma pessoa singular não pode ter uma *expectativa razoável de privacidade* sempre e quando *cede* o seu número de telefone à companhia com a qual efectiva um contrato telefónico (Como? Não é a *companhia-de-telefone* que faculta um número, mediante um contrato assinado entre a empresa e o cliente, para que este utilize e esteja contactável?). Disponível, por exemplo, em: https://supreme.justia.com/cases/federal/us/442/735/case.html . -último acesso Nov.2016
Todavia, felizmente, esta alarvidade jurídica, mesmo do outro lado do Atlântico, começa a ser rebatida. Desde logo, a posição assumida pela Justice Sotomayor no voto que ajudou a formar a maioria de 5-4, no caso UNITED STATES *v.* JONES (2012).
«(...)*More fundamentally,* ***it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.****(...)This approach*

dos pressupostos, pois que esta deveria ser no sentido de, por norma, não se facultar o acesso ao número de telemóvel pessoal (em sentido lato), salvo manifestação inequívoca da vontade do seu titular em sentido contrário. Até porque, obviamente, em sede de preenchimento de um dado *CV,* a cedência de dados pessoais, como sejam o número de telefone, de telemóvel, o *email*, a morada fiscal, entre outros, pressupõem uma finalidade muito própria: o manter formas de contacto privilegiadas entre o titular dos dados e a entidade a quem este cede algumas destas partes do seu todo informacional. Àquela dada entidade em concreto, não ao público em geral[161]. Não obstante, ressalve-se, em abono da verdade, que a Lei n.º 46/2007, de 24 de Agosto, mormente o seu Artigo 3.º, n.º1, alínea b), permitia-se, ao tempo, a esta inaudita interpretação, através da conceptualização absurda de ««*Documento nominativo»* o documento administrativo ***que contenha***, acerca de pessoa singular, identificada ou identificável, ***apreciação ou juízo de valor, ou informação abrangida pela reserva da intimidade da vida privada.***». Curial, ainda assim, sublinhar que esta obtusa formulação foi, entretanto, superada pela entrada em vigor da **Lei n.º 26/2016, de 22 de Agosto**, que passou a conceptualizar ««*Documento nominativo»* ***o documento administrativo que contenha dados pessoais, definidos nos termos do regime legal de proteção de dados pessoais;***[162]».

is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. ***People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.*** *Perhaps, as JUSTICE ALITO notes,* ***some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable,"*** *post, at 10,* ***and perhaps not.*** *I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations,* ***they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.*** *I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.*», Págs. 5 e 6 de UNITED STATES v. JONES SOTOMAYOR, J., concurring. Disponível para consulta, por exemplo, em: https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf . - último acesso Nov.2016.

161 Absurdamente, na lógica da interpretação (outrora) expedida pela C.A.D.A, *ex vi* ponto 12 do sobredito Parecer, «(...)*os elementos constantes do currículo, designadamente o nome,* ***a morada, o número de telefone e de telemóvel,*** *o tempo de serviço e as habilitações/classificações académicas* ***são dados de conhecimento objectivo e, portanto, de acesso generalizado e livre****,* (...)», por auto-censura, para futuro os *CV* apenas passariam a conter a indicação do nome do titular e do seu percurso académico e profissional. Só desta forma, consubstanciando um *despersonalizado* registo biográfico, meramente enunciativo de algumas métricas e/ou critérios para preenchimento de fórmulas matemáticas, qualquer dado pessoal nele constante, se apresentaria *protegido* (omisso, mas protegido) de qualquer tipo de afectação desvantajosa a que pudesse estar sujeito derivada de um cabal e indiscriminado acesso por parte de um qualquer terceiro.

162 Artigo 3.º, n.º1, alínea b) da nova L.A.D.A.

Última nota para relevar a singular interpretação levada a cabo, mormente no ponto 13 do Parecer, pela C.A.D.A. e o *cabal* afastamento da sindicância da queixa em matéria de protecção de dados pessoais[163], propugnado por esta. Mesmo alertada pela entidade requerida para o facto de que «*a utilização de dados pessoais para finalidades não determinantes da recolha depende de autorização da Comissão Nacional de Proteção de Dados (alínea c) do n.º 1 do artigo 23.º da Lei 67/98).»,* a C.A.D.A, ainda assim, justifica que «*Refira-se, a este respeito, que existe um único regime de acesso a documentos administrativos: o regime da LADA (...). E, porque há um só regime de acesso, uma única é também a entidade competente para apreciar as questões emergentes desse direito: a CADA. É, portanto, à luz deste binómio LADA/CADA que a queixa deverá ser analisada.*». Quer uma interpretação integrada, quer sistemática, que esta matéria reclama, é (foi-o geralmente) irremediavelmente desconsiderada[164].

Reconhecendo, *não obstante*, que alguns elementos solicitados se inserem no domínio da vida privada da pessoa, afasta a protecção conferida pelo artigo 26.º, n.º1, da CRP, com uma justificação *legal* pressuposta na distinção entre <u>*vida privada*</u> e <u>*reserva da intimidade da vida privada,*</u> propugnando que os elementos «*não integram, contudo, o núcleo*

163 Mesmo depois da entrada em vigor do RGPD, a 25 de Maio de 2016. Artigo 99.º, n.º1 do RGPD do Regulamento Geral de Protecção de dados, (UE) n.º679/2016, os Pareceres da C.A.D.A, foram mantendo esta tónica interpretativa. Incompreensivelmente.
Atente-se no Considerando(154) do RGPD*: «O presente regulamento permite* ***tomar em consideração o princípio do direito de acesso do público aos documentos oficiais na aplicação do mesmo. O acesso do público aos documentos oficiais pode ser considerado de interesse público****. Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado-Membro que lhes for aplicável.* ***Essas legislações deverão conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor público com o direito à proteção dos dados pessoais e podem pois prever a necessária conciliação com esse mesmo direito nos termos do presente regulamento.*** *A referência a autoridades e organismos públicos deverá incluir, nesse contexto, todas as autoridades ou outros organismos abrangidos pelo direito do Estado-Membro relativo ao acesso do público aos documentos. A Diretiva 2003/98/CE do Parlamento Europeu e do Conselho não modifica nem de modo algum afeta o nível de proteção das pessoas singulares relativamente ao tratamento de dados pessoais nos termos das disposições do direito da União ou do Estado-Membro, nem altera, em particular, as obrigações e direitos estabelecidos no presente regulamento.* ***Em particular, a referida diretiva não deverá ser aplicável a documentos não acessíveis ou de acesso restrito por força dos regimes de acesso por motivos de proteção de dados pessoais nem a partes de documentos acessíveis por força desses regimes que contenham dados pessoais cuja reutilização tenha sido prevista na lei como incompatível com o direito relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais****.»*
164 Uma vez mais, a constância argumentativa para não considerar uma interpretação integradora e sistemática por parte da C.A.D.A, continuou o seu caminho, mesmo depois da consagração expressa do novo Artigo 86.º do RGPD: *«Os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a* ***prossecução de atribuições de interesse público podem ser divulgados*** *pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público,* ***a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais*** *nos termos do presente regulamento.»*

essencial da privacidade, isto é, não cabem no âmbito da reserva da intimidade da sua vida privada. Com efeito, dá-los a conhecer nada dirá sobre "o modo de ser da pessoa", nada dirá que deva ser preservado ou excluído do conhecimento por terceiros. E é por isso que um ***qualquer documento que os refira será, para os efeitos da LADA, um documento administrativo sem conteúdo nominativo,*** *pelo que não existirá - também de acordo com tal lei - qualquer obstáculo ao acesso por terceiros (sejam eles particulares, sejam entes públicos).* ***E, tratando-se de um documento administrativo desprovido de caráter nominativo, não se levanta a questão de saber se converge (ou não) na requerente um interesse direto, pessoal e legítimo****.»*[165] . Interpretação, uma vez mais, ainda que *legalmente* sustentável, juridicamente inadmissível, por uma completa inaptidão interpretativa, completamente omissa quanto à integração e sistematização da matéria considerada, conducente a uma perigosa desconsideração e despersonalização da pessoa singular titular dos dados. Estivesse o foco deste pleito considerado na pessoa singular e não nos seus dados e, queremos acreditar, o douto entendimento sufragado teria sido, necessariamente, diverso.

B) – O Parecer n.º 36/2016

Por sua vez, no Parecer n.º 36/2016, «*"Por suspeita de irregularidades", a Associação de Pais e Encarregados de Educação do Agrupamento de Escolas (...) (AP) solicitou ao Centro de Estudos Judiciários (CEJ) que lhe fossem "facultados os documentos entregues"* (...)» por uma dada pessoa singular, candidata ao exercício da Actividade de Administrador Judicial, cujo concurso fora promovido pelo CEJ.

Neste caso, em particular, a entidade requerente AP, uma vez concretizada a *"indicação precisa dos documentos que pretendia",* solicitou ao CEJ o acesso à informação daquela dada pessoa em concreto, nomeadamente, ao «-*"Curriculum vitae"; - "Declaração sobre o exercício de qualquer outra atividade remunerada e sobre a inexistência de qualquer das situações de incompatibilidade previstas na lei"; - "Declaração de idoneidade"; - "Declaração da sua situação financeira, com a discriminação de proveitos auferidos e encargos suportados à data da Declaração"; - "Qualquer outro documento que o candidato tenha considerado relevante para a instrução da sua candidatura, nomeadamente de desempenho, se houver"; - "Um esclarecimento sobre a participação"*

165 Pontos 15 e 16 do Parecer.

daquela pessoa "em sociedades comerciais alvo de insolvência (...)». A C.A.D.A, uma vez instada a pronunciar-se, volta a insistir no argumentário expendido, em sede de admissibilidade do acesso irrestrito à informação constante do *CV*, e já sumariamente analisado no Parecer anterior. Não de somenos, cumpre-nos salientar a erraticidade do argumento utilizado relativamente a este tipo de acesso - indiscriminado, sem necessidade de justificação nem interesse directo e legítimo.

Assim, objectivando a crítica que pretendemos salientar, a C.A.D.A, reconhecendo que «*"(...) um curriculum vitae conterá referências ao nome e à morada.(...)*"», prossegue nos argumentos com «*"(...) embora o nome e a morada sejam dados pessoais, os documentos administrativos que os contenham não são «documentos nominativos» para os efeitos dos arts. 3.º, n.º 1, al. b), e 6.º, n.º 5, da Lei n.º 46/2007, de 24/8,"»*. Salientando que «"*O curriculum vitae inserirá, igualmente, os números de telefone e de telemóvel."*»[166], ainda assim, justifica a admissibilidade de acesso a todos estes dados pessoais, sem qualquer tipo de consentimento expresso por parte do seu titular, apenas e só por manifesta teimosia identitária em não fazer uma leitura integradora e sistemática do regime jurídico da matéria em contenda. A bipolaridade desta singular interpretação, risivelmente, expressa-se, pelo cunho da própria entidade, através da assumpção de que: «*Se há pessoas que pedem que a sua morada e/ou o seu número de telefone, se tornem ou mantenham confidenciais, fazem-no para não serem incomodadas por uma dessas vias. É um direito que lhes assiste e que cumpre respeitar. Portanto, desde que não haja oposição expressa ao conhecimento por terceiros dos telefones, nada obsta à sua disponibilização."*»[167]. *Lapidar*, novamente, nas conclusões. Mesmo que completamente errada nos pressupostos, uma vez que a interpretação deve ser no sentido precisamente oposto de que por regra não se faculta o acesso ao número de telemóvel (telefone, *email*, morada) pessoal, salvo manifestação inequívoca da vontade do seu titular em o facultar. Precisamente para as pessoas titulares destes dados *não serem incomodadas por uma dessas vias.* Insistimos, o foco deste tipo de pleito deveria ter incidido sempre sobre a pessoa, singular, e não sobre a natureza mais ou menos *nominativa*, mais ou menos *administrativa* dos seus dados pessoais.

166 Ponto 11 do sobredito Parecer.
167 *Idem.*

4.3.1.2 – O *VOLTE-FACE*. O PARECER N.º 425/2016 [168]

A *doutrina* da C.A.D.A, neste breve excurso de que fomos dando conta no ponto anterior, acabaria, *contudo*, por revirar *numa lufada de ar fresco* com a entrada em vigor da nova L.A.D.A.. Salientamos, desde logo, a redacção (clarificadora) da definição de documento nominativo[169]: *«o documento administrativo que contenha dados pessoais, definidos nos termos do regime legal de proteção de dados pessoais;».* Mas, igualmente, no campo das clarificações conceptuais, também a definição de documento administrativo[170], de que já demos conta, foi refeita.

Se uma das principais deficiências do anterior regime legal apontava precisamente para o sentido hermético (nada integrador muito menos sistemático) que a definição de «*documento nominativo*» emprestava à interpretação, *sui generis*, que a C.A.D.A. foi desenvolvendo ao longo da vigência da anterior L.A.D.A, com o novo regime legal, o legislador entendeu, por bem, *aclarar* o conceito. Despida desse *dogmatismo anterior*, como veremos, a doutrina da C.A.D.A., passou a considerar a necessidade de uma *interpretação integradora e sistemática* - até então completamente omissa - reveladora do *equilíbrio que o legislador quis* considerar *na aplicação de cada uma das leis – LADA e LPDP,* efectivando, por conseguinte, uma *ponderação da natureza da informação em causa e as circunstâncias concretas do caso*[171] concreto. Mas, sublinhe-se, não seria esta *interpretação integradora e sistemática* necessária por si só, *ab initio*, mesmo na vigência do anterior regime, que se exigiria que a entidade administrativa levasse em consideração?

Uma vez analisado o Parecer *sub judicio,* correctamente, a C.A.D.A entendeu que *o conceito de informação nominativa contido na LADA obriga à sua articulação com o disposto na LPDP*[172]. Ainda assim, mesmo que o voltasse a omitir, decorreria sempre –

168 Disponível em: http://www.cada.pt/uploads/Pareceres/2016/425.pdf . - Último acesso Nov.2016.
169 Artigo 3.º, n.º1, alínea b) da, nova, L.A.D.A..
170 Assim, Artigo 3.º, n.º1, alínea a) da, nova, L.A.D.A: ««*Documento administrativo» qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detido em nome dos órgãos e entidades referidas no artigo seguinte, seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a: i) Procedimentos de emissão de atos e regulamentos administrativos; ii) Procedimentos de contratação pública, incluindo os contratos celebrados; iii) Gestão orçamental e financeira dos órgãos e entidades; iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas.»*
171 Ponto 12 do Parecer n.º 425/2016.
172 Ponto 18 do Parecer.

como na altura da vigência do anterior regime legal - uma exigência constitucional de protecção do acesso aos dados pessoais por terceiros, *ex vi* artigo 35.º, n.º4, da CRP. Não olvidando, todavia, *a estrutura de direito liberdade e garantia do artigo 268.º, n.º2*[173], da CRP, que tutela o direito de acesso à informação administrativa - bitola pela qual se rege a C.A.D.A - não deixa de ser uma *feliz novidade,* a constatação da inflexão da doutrina expendida por esta entidade. Com efeito, na ponderação casuística, concreta, levada a cabo, a C.A.D.A, avaliando da ***natureza nominativa dos documentos em causa*** [artigo 3.º, n.º 1, alínea b)], bem como da incidência das **pretensões de um requerente *sem autorização escrita dos titulares dos dados***; ***sem invocar a necessidade de acesso à documentação em causa***; e, em consequência, também ***não demonstra ser portador "de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação"***[174], decidiu-se a ***denegar*** – e bem – ***o acesso aos documentos pretendidos.*** Seguramente que, se a decisão tivesse sido tomada à vigência do anterior regime, a C.A.D.A, ter-se-ia decidido pela necessidade de transmissão da informação sem a necessidade de indicação de qualquer razão justificativa do acesso. Contudo, e finalizando, felizmente o legislador, em 2016, decidiu-se a dissipar o *nevoeiro legal* por onde esta entidade se movia.

173 C.R.P. - *«Artigo 268º- Direitos e garantias dos administrados: (...) 2. Os cidadãos têm também o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas.»*
174 Pontos 19 e 20 do Parecer.

4.4. O PARADOXO DE SEGURANÇA NA DISPONIBILIDADE DA AUTORIDADE TRIBUTÁRIA E ADUANEIRA EM PORTUGAL

Reservamos um espaço, destacado, para apreciação do poder, *disruptivo,* privilegiado, que já hoje a Autoridade Tributária e Aduaneira detém em matéria de acesso e tratamento de dados pessoais. Neste conspecto, é pois necessário trazer à colação a apreciação crítica desenvolvida pela CNPD, por exemplo, quando instada a pronunciar-se quanto à proposta de lei[175] do Orçamento de Estado para 2016, vertida no Parecer n.º 5/2016[176], bem como aquando da apreciação da proposta de lei do Orçamento de Estado para 2017[177], através do Parecer n.º 43/2016[178].

4.4.1. AS TENSÕES E A PRIMAZIA DA LEI FISCAL SOBRE OS DIREITOS, LIBERDADES E GARANTIAS DA PESSOA

É inegável a sucessiva e crescente interconexão do sistema de informação da Autoridade Tributária e Aduaneira (doravante, AT) com os outros sistemas de informação da Administração Pública. No Parecer n.º5/2016, por exemplo, a transmissão, acesso e interconexão de dados entre a AT, a Segurança Social e a Caixa Geral de Aposentações (doravante, CGA), I.P., foi objecto de apreciação crítica. E por estarmos em presença de *interconexão* de dados entre serviços do Estado, relativos a «*rendimentos e regimes contributivos*», parece-nos óbvia a argumentação expendida, no aludido parecer, no sentido de uma maior clarificação dos normativos analisados. Com efeito, a *deficiente* redacção de normas, pejadas de conceitos vagos e indeterminados, permite uma *miríade* de interpretações, regra geral densificadas por circulares internas, que extravasam larga e desvantajosamente o objecto inicial do legislador, superando a salvaguarda dos direitos fundamentais da pessoa em nome da eficiência fiscal, *divina, que cumpre efectivar*.

175 Proposta de Lei n.º12/XIII/1ª (GOV). Disponível para consulta *online* em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a53556b76644756346447397a4c334277624445794c56684a53556b755a47396a&fich=ppl12-XIII.doc&Inline=true - último acesso Nov.2016.
176 Disponível em: https://www.cnpd.pt/bin/decisoes/Par/40_5_2016.pdf . - último acesso Nov.2016.
177 Proposta de Lei n.º37/XIII/2ª (GOV). Disponível para consulta *online* em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795a5868774d546f334e7a67774c336470626d6c7561574e7059585270646d467a4c31684a53556b76644756346447397a4c33427762444d334c56684a53556b755a47396a&fich=ppl37-XIII.doc&Inline=true - último acesso Nov.2016.
178 Disponível em: https://www.cnpd.pt/bin/decisoes/Par/40_43_2016.pdf . - último acesso Nov.2016.

Outro aspecto que cumpre relevar prende-se com a sindicância feita pela CNPD à norma prevista no artigo 170.º desta proposta de lei[179]. Compreendemos a *bonomia* pressuposta na necessidade de uma maior *eficiência fiscal* que o Estado procura atingir. De facto, no

179 *«Artigo 170.º Autorização legislativa para acesso e troca de informações financeiras:*

1 - Fica o Governo autorizado a proceder à transposição para a ordem jurídica nacional da Diretiva 2014/107/UE, do Conselho, de 9 de dezembro de 2014, que altera a Diretiva 2011/16/UE no que respeita à troca automática de informações obrigatória no domínio da fiscalidade, e a estabelecer o regime para a troca de informações de contas financeiras ao abrigo de convenções internacionais, em observância da Norma Comum de Comunicação (CRS) desenvolvida pela Organização para a Cooperação e Desenvolvimento Económico (OCDE), bem como a prever que as regras de comunicação à Autoridade Tributária e Aduaneira e de diligência devida sejam aplicadas pelas instituições financeiras relativamente a contas financeiras qualificáveis como sujeitas a comunicação nos termos da Diretiva 2014/107/UE e da CRS.

*2 - **Fica ainda o Governo autorizado a estabelecer a obrigatoriedade de comunicação à Autoridade Tributária e Aduaneira** e de cumprimento dos procedimentos de diligência devida, em termos equivalentes aos previstos nos instrumentos jurídicos a que se refere o número anterior, em relação às contas financeiras qualificáveis como sujeitas a comunicação, mantidas por instituições financeiras reportantes e cujos titulares ou beneficiários efetivos sejam residentes no território nacional.*

*3 -**O sentido e a extensão das autorizações legislativas** previstas nos números anteriores são os seguintes:*

a) Alterar as regras e os procedimentos de cooperação administrativa no domínio da fiscalidade previstos no Decreto-Lei n.º 61/2013, de 10 de maio, compreendendo, nomeadamente: i) Estabelecer uma cooperação administrativa mútua mais ampla entre a Autoridade Tributária e Aduaneira e as autoridades competentes de outros Estados-membros ou de outras jurisdições no âmbito de convenções internacionais, no que se refere à troca automática de informações de contas financeiras; ii) Limitar a troca automática obrigatória de informações de contas financeiras com jurisdições que não pertencem à União Europeia àquelas que assegurem um nível de proteção adequado de dados pessoais; iii) Alargar o mecanismo de troca automática de informações para finalidades fiscais, tendo por base uma abordagem coerente e uniforme com o Regime de Comunicação de Informações Financeiras, aprovado pelo artigo 239.º da Lei n.º 82-B/2014, de 31 de dezembro, de modo a minimizar os custos para as instituições financeiras abrangidas e para a administração tributária; iv) Definir o âmbito das informações abrangidas pela troca obrigatória e automática com as autoridades competentes de outros Estados-membros ou de outras jurisdições no âmbito de convenções internacionais, no que se refere à troca automática de informações de contas financeiras; v) Aplicar as soluções adotadas pela Diretiva 2014/107/UE para efeitos de seleção das opções previstas na CRS; vi) Adotar opções comuns para efeitos da Diretiva 2014/107/UE e da CRS, prevendo as soluções que, assegurando a fiabilidade da informação recolhida e comunicada, se revelem mais flexíveis e menos onerosas na perspetiva das instituições financeiras;

b) Rever e adaptar a legislação fiscal, nomeadamente a Lei Geral Tributária, aprovada pelo Decreto-Lei n.º 398/98, de 17 de dezembro, de modo a consagrar, em condições equivalentes às previstas na Diretiva 2014/107/UE, bem como nas convenções internacionais assinadas pela República Portuguesa que prevejam troca de informação financeira e fiscal, a obrigatoriedade de cumprimento das regras de comunicação e diligência devida em relação às contas financeiras qualificáveis naquelas como sujeitas a comunicação, independentemente da residência do respetivo titular ou beneficiário;

c) Consagrar exigências específicas em matéria de recolha, conservação e transmissão de dados, garantindo a observância dos direitos fundamentais em matéria de proteção de dados pessoais;

d) Rever os ilícitos previstos no Regime Geral das Infrações Tributárias, aprovado pela Lei n.º 15/2001, de 5 de junho, de modo a prever penalidades para as infrações decorrentes do incumprimento das obrigações de comunicação ou de diligência devida por parte das instituições financeiras a estas sujeitas, bem como da obrigação de manutenção de registo e de elementos comprovativos que tenham servido de base à obtenção das informações e à execução dos procedimentos de comunicação e diligência devida;

e) Rever o Regime Complementar do Procedimento da Inspeção Tributária e Aduaneira, aprovado pelo Decreto-Lei n.º 413/98, de 31 de dezembro, dotando a Autoridade Tributária e Aduaneira dos poderes adequados à verificação do cumprimento das obrigações previstas neste âmbito.»

presente, ante uma realidade nacional de crescimento económico anual anémico - cujas perspectivas futuras pouco ou nada aparentam mudar - só uma maior eficácia tributária, numa *eficiente* arrecadação de receitas por via de impostos, permitirá que os Governos possam ir remendando as contas gerais anuais do Estado. Logo, este tema da eficiência fiscal – a qualquer custo, em abono da verdade – é tema *tabu* no seio dos partidos do arco da governação. Não obstante, não compreendemos, nem tampouco cedemos, quanto ao meio utilizado para alcançar esse fim – a pessoa.

No caso português, a essência da nossa república soberana e a marca genética do Estado de Direito Democrático assina pelo nome de dignidade da pessoa humana. Esta base encontra respaldo logo no artigo 1.º da CRP. Assumindo-se como pilar da nossa identidade, causa-nos a maior desconfiança a importação, por exemplo, do outro lado do Atlântico, do *nothing to hide argument*[180]. Pior ainda quando, ao longo dos anos mais recentes de superação económica a qualquer custo, têm-nos sido presentes as *maravilhas* de conversão da pessoa num número único. Pela facilidade, economia, e objectividade da transformação, a pessoa, *acometida a um all-in-once object,* permite, por um lado, um *relacionamento* mais eficiente Pessoa-Estado, e, por outro lado, uma baixa no custo desse seu relacionamento, permitindo uma *eficiente desobstrução de processos*. Surreal.

Recuperando o aludido Parecer n.º 5/2016, entre outras conclusões, e sindicando a norma desse Artigo 170.º, cumpre-nos destacar a intransigência operada pela CNPD na defesa dos direitos, liberdades e garantias fundamentais da pessoa. Uma vez mais, como veremos, o poder político procura concretizar no ordenamento jurídico nacional os *procedimentos de diligência devida, assim como a norma comum de comunicação (CRS) desenvolvida pela OCDE,* transpondo a Directiva 2014/107/UE, do Conselho, de 09 de Dezembro de 2014. Por sinal, já em 2014, no Parecer n.º 58/2014[181], a mesma CNPD

180 A divinização do ***nothing to hide argument***, pressuposta na *eficiência.* Este tipo de argumento – originário de outras latitudes menos garantísticas – encontra respaldo no seguinte silogismo, básico: *«Se eu não tenho nada a esconder; Se eu não tenho nada a temer; Logo não devo ter preocupações quanto à defesa da minha privacidade».* Pode parecer sedutor. Porém, esta *eficiência* contende directamente com direitos, liberdades e garantias fundamentais das pessoas. E se estes conferem a disponibilidade de a pessoa poder ter o direito a segredos, então, salvo razões constitucionalmente inadiáveis, a pessoa tem de poder ter o direito ao segredo. Ao sigilo. À confidencialidade. Ou defendemos e somos intransigentes na defesa de um direito ao segredo, ou cedemos, e de forma translúcida apresentamo-nos *despidos* ante o aparelho estatal.

181 Disponível *online* para consulta em : https://www.cnpd.pt/bin/decisoes/Par/40_58_2014.pdf . - último acesso Nov.2016.

tinha concluído, liminarmente, pela sua não concordância quanto à – suposta - primazia da *legislação fiscal* sobre a legislação nacional relevante em sede de dados pessoais de natureza sensível. Nessa decisão, a falta de mecanismos que garant(i)am o sigilo e a confidencialidade do tratamento dos dados, bem como a possibilidade – não europeia – de troca de informações exercida de forma automática, e, *com recurso a prestadores de serviços externos,* suscitaram de imediato uma forte reprovação por parte da CNPD. Não obstante, a exportação – e imposição - americana do mecanismo FATCA *(Foreign account tax compliance Act)* tem voltado, numa constância assinalável, à berlinda[182].

Em nome da economia e objectivação do presente excurso, acompanhamos a pertinência das objecções propugnadas pela CNPD. Com efeito, *sendo já do conhecimento da AT os rendimentos de capitais e as mais-valias originadas por venda ou resgate de ativos financeiros, (...), a novidade ficará, na prática, reduzida ao conhecimento dos saldos de conta – desde logo, de depósito – no final de cada ano civil ou de outro período considerado adequado para o encerramento de contas.* O que, como resultado, projecta uma restrição ao direito à protecção de dados pessoais, consagrado constitucionalmente no artigo 35.º da CRP, que extravasa os limites de constitucionalidade admissíveis para restrição de um direito, liberdade ou garantia, ao arrepio do princípio da proporcionalidade, sedeado no artigo 18.º, número 2, da CRP[183].

Pelos vistos, a complexa teia de poderes – e de conhecimento - que já hoje a AT tem à sua disposição, parece ser *curta*. Pelo menos, para o apetite estadual. Só assim se explica a necessidade de, em suposto nome da *prevenção e combate à evasão fiscal*, o Estado pretender alargar – ainda mais – esse vasto leque de competências da AT. Errado nos motivos, porquanto, completando uma inadmissível inversão do ónus da prova, o Estado assume cada um dos seus cidadão como prevaricadores. É neste sentido que a conclusão da CNPD arrasa o propósito da sugestão legal contida nesse Artigo 170.º dessa Proposta de lei: *«(...)não sendo o conhecimento de saldos de conta per se uma medida apta a prevenir ou combater o incumprimento de obrigações fiscais, uma vez que aqueles não estão sujeitos a tributação. Por outro lado, tal medida implica uma restrição de tal forma*

182 *Vide*, por exemplo, Plano de actividade 2016, da Autoridade Tributária e Aduaneira, disponível *online* em:http://info.portaldasfinancas.gov.pt/NR/rdonlyres/4552CA90-2467-4CC7-83B5-A9A0B0942C31/0/PA_2016.pdf - último acesso Nov.2016.
183 Conforme se pode ler no Parecer *sub judicio*.

generalizada do direito à protecção de dados pessoais e do direito à reserva da vida privada de todos os titulares e beneficiários de contas, que a mera previsão da possibilidade da sua imposição sempre obrigaria o legislador a demonstrar que não existem medidas menos lesivas, quanto à intensidade ou ao âmbito, da esfera jurídica dos cidadãos para alcançar a mesma finalidade(...)». Seguramente que o caminho, no combate à evasão fiscal, não deverá ser feito tomando todas as pessoas como *criminosos fiscais,* imputando-lhes o ónus de provarem que não o são.

Cumpre-nos agora relevar o Parecer n.º 43/2016. Versando sobre a Proposta de Lei n.º37/XIII/2ª (GOV), analisado o sobredito, notamos a constância – crescente - na interconexão das mais variadas bases de dados da administração pública estatais com o gigante silo de dados pessoais da AT. No parecer *sub judicio*, damos conta da interconexão das bases de dados dos serviços da administração interna e do planeamento de infraestruturas com competência na área do direito rodoviário contra-ordenacional (artigo 84.º da Proposta[184]), e das da Segurança Social e da Autoridade para as Condições do Trabalho (ACT) (artigo 127.º da Proposta[185]), entre outras, afunilando (pelo menos, propondo) tal interconexão no *sistema de informação da AT, na "base de dados centralizada" da Administração Pública portuguesa, em nome da eficiência administrativa*.

---

184 *«Artigo 84.º Interconexão de dados no âmbito das contraordenações rodoviárias*

1 - Com vista a melhorar a eficácia dos processos de contraordenações rodoviárias, o Governo pode estabelecer a interconexão de dados entre os serviços da Autoridade Tributária e Aduaneira e os serviços da área da administração interna e do planeamento e das infraestruturas com competências na área do direito contraordenacional rodoviário, por forma a facilitar o acesso aos dados registados na administração fiscal que sejam relevantes para instauração e tramitação dos processos.

2 - As categorias dos titulares e dos dados a analisar, bem como o acesso, a comunicação e o tratamento de dados entre as entidades referidas no número anterior realiza-se nos termos de protocolo estabelecido entre os membros do Governo responsáveis pelas áreas das finanças, da administração interna e do planeamento e das infraestruturas, sujeito a autorização da Comissão Nacional de Proteção de Dados.»

185 *«Artigo 127.º Interconexão de dados entre a administração fiscal, a segurança social e a Autoridade para as Condições do Trabalho*

1 - Com vista a melhorar a eficácia do combate às infrações laborais e promover a efetividade do direito laboral, o Governo pode estabelecer a interconexão de dados entre os serviços da Autoridade Tributária e Aduaneira, da Segurança Social e da Autoridade para as Condições do Trabalho, por forma a facilitar o acesso aos dados registados na administração fiscal e na segurança social relevantes para a realização das inspeções laborais, com o objetivo de assegurar o controlo do cumprimento do normativo laboral no âmbito das relações laborais e a promoção da segurança e saúde no trabalho em todos os setores de atividade.

2 - As categorias dos titulares e dos dados a analisar, bem como o acesso, a comunicação e o tratamento de dados entre as entidades referidas no número anterior realiza-se nos termos de protocolo estabelecido entre os membros do Governo responsáveis pelas áreas das finanças, do trabalho e da segurança social, sujeito a autorização da Comissão Nacional de Proteção de Dados.»

Novamente, crítica transversal a ambas as propostas de Lei, começaremos por destacar a insistência legislativa em disposições de carácter vago, cujos normativos carecem de necessária densificação. Por acto legislativo. Já o referenciámos anteriormente, mas, registe-se que, contrariando a prática institucional *contra legem* - cuja *miríade* de interpretações vertidas em circulares internas pretendemos erradicar – acompanhamos (obviamente) o entendimento expedido pela CNPD neste Parecer. Com efeito, «*no domínio dos direitos, liberdades e garantias, exige-se, pois, com «particular acuidade» às normas legais que contenham os elementos que lhes permitam operar como normas de actuação para a administração e «normas de controlo», devendo os termos concretos da intervenção administrativa constar de lei «[não sendo] legítimo que dependam de um juízo de oportunidade e conveniência da própria autoridade administrativa, não previsível ou mensurável pelos particulares, nem controlável (senão negativamente) pelos tribunais.»* Naturalmente.

De igual forma, ponto de, óbvia, discórdia é a interconexão de variadas bases de dados da Administração Pública com esse grande silo da AT. Em sede de análise do artigo 84.º da Proposta, a CNPD (re)lembra o carácter desnecessário da interconexão da base de dados da administração interna e do planeamento de infraestruturas com competência na área do direito rodoviário contra-ordenacional com o silo da AT, precisamente por entender que, se a finalidade objectivada pelo Governo passaria por, para efeitos de instauração e tramitação de processos de contra-ordenação rodoviária, fazer coincidir o dado pessoal morada (residência) com o domicílio fiscal, a Base de Dados de Identificação Civil (BDIC) mostra-se como alternativa suficiente e menos lesiva para tal propósito, considerando-se a interconexão com esse silo da AT como violador do *princípio da proporcionalidade, por evidente falta de necessidade.*

Quanto ao artigo 127.º, começando por evidenciar a pouca compatibilidade – em termos de tratamento de dados pessoais - que poderá existir da interconexão das bases de dados da Segurança Social e da ACT com o grande silo da AT, a CNPD infirma ainda que *não (se) consegue adivinhar que dados pessoais, dos que existem nas bases de dados da AT ou da Segurança Social, permitem inspeccionar as condições de trabalho ou melhorar a eficácia do combate às infrações laborais.* E se é indesmentível que, ano após ano, *na*

verdade, o que o legislador nacional tem sucessivamente vindo a fazer, nas duas últimas décadas, é resolver as necessidades de eficiência da Administração Pública no acesso a informação sobre os administrados com recurso aos sistemas de informação da AT, o caminho da cristalização de uma base de dados centralizadora, única, aparece-nos como epílogo de todas estas estaduais tentativas – em nome da eficiência e contenção de custos - de numeração única da pessoa. O tratamento, cruzamento e mapeamento da identidade informacional completa da pessoa, num único registo, na disposição da Autoridade Tributária e Aduaneira, fundado n*a fidedignidade aí conservada* (no silo da AT)*, mas também no extenso leque de dados pessoais relativos aos cidadãos que a AT hoje conserva,* deveria fazer-nos suscitar as maiores críticas. Mas todas estas conclusões, óbvias, são negligenciáveis para *a polis* e respectivo exercício do poder político.

Acresce que, nos mais variados segmentos do aparelho do Estado, é *firme* a apologia de modernidade tecnológica onde o espaço para o medo das *extraordinárias possibilidades que a capacitação tecnológica* permite, simplesmente não existe. O *idílico espaço* desta digital administração pública afunila cada vez mais no tal grande silo(s) da Autoridade Tributária; o qual por sua vez, não concede, em tempos de recursos económicos contingentes, espaço para o *desperdício* de dinheiros públicos na manutenção de diferentes alternativas (bases) de dados pessoais pelas diferentes estruturas da Administração Pública. O custo que esta manutenção encerra representa uma oneração, *desnecessária e desvantajosa*, para o Estado. Daí que, invectivando uma *visão táctica e estratégica*, racional, eficiente e economicista (acrescento nosso), a necessidade de um número identificador único, para cada pessoa, se revele como decisiva: «*Uma identificação única aumenta a qualidade dos dados*»[186]…Resta saber, aumenta a *qualidade* «*para quê*»? Tal e qual o princípio vertido na CRP, no seu artigo 35.º, n.º1 – o princípio da finalidade - ordena. Não obstante, questionamos, ainda que de forma retórica – em sede de tratamento de dados pessoais –, se o consentimento dado pela pessoa titular dos dados a uma entidade pública (ou privada) permite - para um ulterior tratamento de dados - a sua posterior confluência nesse único silo da AT.

186 Palavras proferidas por Luís Vidigal, especialista do Instituto de Informática do Ministério das Finanças no âmbito da «*Conferência Prós e Contras da aplicação do Artº 35º da Constituição*». Lido e revisto o sumário, parece-nos, de facto, salvo raras excepções, *extenuante*, o resultado apresentado e publicado pela APDSI, em 2008, no contexto da dita conferência. Disponível *online* em: http://www.apdsi.pt/uploads/news/id183/relato.pdf . -último acesso Nov.2016.

A forte e imediata possibilidade – pela permissividade e laxismo que a prática permite - de transformação da pessoa em mero objecto de informações, em jeito *orwelliano*, encerra na concretização desta num número, único, identificador pessoal, o seu risco mais nefasto. Desde logo, para a salutar manutenção do Estado de Direito Democrático que conhecemos. A consumação desta base de dados única, mais *económica* para os cofres gerais e mais «*amiga*» destes mesmos cofres, contende – largamente – com a proibição constitucional vertida no artigo 35.º, n.º 5 da CRP[187]. E se o risco de uma visão única e totalitária da pessoa é real, *assim como assim*, o paradoxo de segurança em que se esconde, apenas o confirma. Neste paradoxo, o Estado, *paternalista*, para sua manutenção e prossecução futura, insiste na necessidade de uma visão da pessoa (seus filhos) despida de *segredos*. Só assim este Estado, *paternalista,* lhe poderá garantir um espaço de segurança.

E, se é certo que, secundando a opinião expressa por José Alberto Vieira[188], a tensão presente de escolha entre *considerar mais importante a facilidade administrativa ou a defesa de liberdades e garantias, encerra uma opção civilizacional*, uma primazia pela lei fiscal em detrimento do regime constitucionalmente consagrado dos direitos, liberdades e garantias, diz muito da sociedade que temos vindo a criar. Com efeito, na alvorada da digitalização de tudo, o estado da arte –de pendor estatal - tem relativizado numa unicidade comprometedora a arte dos estados singulares de cada pessoa. E assim, o peso da expressão de Otto Gritschneder[189], sintomaticamente deveria fazer-nos despertar da presente dormência : «*Wer in der Demokratie schläft, wacht in der Diktatur auf*», i.e., aquele que adormece na luta pela democracia, poderá acordar numa ditadura.

187 Fica um registo de uma tomada de posição da APDSI, em 2011, a propósito da proibição constitucional do Artigo 35.º, n.º5. Disponível para consulta *online* em: http://www.computerworld.com.pt/2011/02/01/apdsi-volta-a-reclamar-fim-do-numero-nacional-unico/ . -último acesso Nov.2016.

188 Ainda a «Conferência Prós e Contras da aplicação do Artº 35º da Constituição», da APDSI, em 2008. Disponível *online* em: http://www.apdsi.pt/uploads/news/id183/relato.pdf . -último acesso Nov.2016.

189 Autor de «*Furchtbare Richter. Verbrecherische Todesurteile deutscher Kriegsgerichte*». (Terrível Juiz. Crimes de sentenças de morte de tribunais marciais alemães), em entrevista a Die Gazette, nr.8, November 1998, disponível *online* em: http://www.gazette.de/Archiv/Gazette-8-November1998/Interview.html . -último acesso Nov.2016.

5. O REGULAMENTO GERAL DE PROTECÇÃO DE DADOS (RGPD[190])

Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da união, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica[191]. Com efeito, entre dificuldades de harmonização de ordem variada, deficiências jurídicas da DPD entretanto complementadas por via jurisprudencial, avanços (significativos) tecnológicos, e um mercado único digital para a Europa (em vista no H2020), entre outros, as instâncias europeias foram compelidas a avançar no sentido da materialização do "*privacy package*"[192], apresentado pela Comissão Europeia em 2012. O contexto europeu apresenta(va) 28 (eventualmente, a caminho de 27) legislações diferentes, no tocante à protecção de dados. Esta *desarmonia* legal, em especial, espelha vicissitudes várias que constituem sérios entraves ao desenvolvimento das empresas, dos seus negócios, bem como a um pleno exercício dos direitos dos titulares dos dados pessoais. É, pois, neste contexto que, a 04 de Maio de 2016, é, finalmente, publicado, no Jornal oficial da União

190 Em inglês, *General Data Protection Regulation* (GDPR).

191 Considerando (9) do RGPD.

192 Este "*Privacy Package*", em traços gerais, salientava a necessidade de um Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a protecção de dados) bem como de uma Directiva do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados. «*The core of the data protection reform package consists of: – a Regulation replacing Directive 95/46/EC; – a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, detection, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. These legislative proposals are accompanied by a report on the implementation by Member States of what is currently the main EU data protection instrument in the areas of police cooperation and judicial co-operation in criminal matters, the Framework Decision 2008/977/JHA*», *in* **COM(2012) 11 final 2012/0011 (COD)**, pág.104. Disponível em: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. – Último acesso Set.2016

Europeia, o *pacote legislativo*[193] derivado daquela iniciativa de proposta de reforma de 2012 da Comissão[194].

Pela nossa parte, embora reconhecendo a transversalidade do tema da protecção de dados e dos instrumentos jurídicos publicados que aqui fazemos referência, focar-nos-emos, em especial, no Regulamento (UE) 2016/679 Do Parlamento Europeu E Do Conselho de 27 de abril de 2016, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (*Regulamento Geral sobre a Proteção de Dados*).

5.1. DO ALARGAMENTO MATERIAL E TERRITORIAL DO ÂMBITO DE APLICAÇÃO DAS NOVAS REGRAS

O RGPD entrou em vigor no dia 25 de maio de 2016[195]. Concedendo um prazo de três (3) anos para que a sociedade proceda às adaptações necessárias até à sua efectiva aplicação[196], certo é que a partir de partir de 25 de maio de 2018 a protecção de dados na U.E. passará a ser uma disciplina unívoca no quadro de todos os seus E.M.

5.1.1. Neste sentido, cumpre relevar aspectos, alguns, que concentrarão as atenções e acções quotidianas no futuro. O RGPD apresenta um espectro, *largo*, de aplicação material. Aplicando-se *ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais*

193 Corresponde ao (i) *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*; (ii) *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho*; e, adicionalmente, (iii) *Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave*. Publicação disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT. – Último acesso Set.2016

194 Com efeito, esta vontade, em abono da verdade, e após algumas críticas de inaptidão aos tempos novos da Directiva de protecção de dados de 1995, poderá retroagir a 2010, à Comunicação IP/10/1462 de 4 Novembro 2010, disponível em: http://europa.eu/rapid/press-release_IP-10-1462_pt.htm – último acesso Set.2016.

195 Artigo 99.º, n.º1, do RGPD. «(…)*vigésimo dia seguinte ao da publicação*(...)»

196 Artigo 99.º, n.º2, do RGPD. «(…) *25 de Maio de 2018*(…)».

contidos em ficheiros ou a eles destinados[197]*,* seja por entidades que tratem directamente dados pessoais, através da realização de operações que os envolvam, seja por entidades que efectuem essas operações em regime de subcontratação. Exime-se (da aplicação), compreensivelmente, nos casos previstos nas alíneas a) a d), do n.º2, do Artigo 2.ºdo RGPD[198], ainda que a expressão «*incluindo(...) a prevenção de ameaças à segurança pública*»[199] na parte final da alínea d), desse n.º2, do artigo 2.º , nos convoque, em acto contíguo, para o risco do "*direito penal do risco"*[200].

5.1.2. No que concerne ao seu âmbito de aplicação espacial, o RGPD, acolhendo recente jurisprudência[201] do TJUE, apresenta-a como *novidade*. Aplicando-se de forma uniforme *em todo o território da União, independentemente de o tratamento ocorrer dentro ou fora da União*[202]*,* prevê a sua aplicabilidade aos casos em que as organizações, que procedam ao *tratamento de dados pessoais de titulares residentes no território da União*, *mesmo*

197 Artigo 2.º, n.º1, do RGPD.

198 Relevando, por sinal, a clarificação entretanto operada pela jurisprudência do TJUE, no caso, a começar pelo *Acórdão Lindqvist, PROCESSO C-101/01, de 6/11/2003*. *Vide*, ainda, *Considerando (18) «O presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.*».

199 *Vide,* a este propósito, o caso americano envolvendo a empresa *Geofeedia*. «*Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color. The ACLU of California has obtained records showing that Twitter, Facebook, and Instagram provided user data access to* ***Geofeedia, a developer of a social media monitoring product that we have seen marketed to law enforcement as a tool to monitor activists and protesters****. We are pleased that after we reported our findings to the companies, Instagram cut off Geofeedia's access to public user posts, and Facebook has cut its access to a topic-based feed of public user posts. Twitter has also taken some recent steps to rein in Geofeedia though it has not ended the data relationship.(...).*» Disponível em: https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target - Último acesso Out.2016.

200 Gomes CANOTILHO apresenta uma crítica contundente. «*Uma coisa é falar-se dos problemas de risco típico da civilização tecnológica (riscos químicos, atômicos, medicamentosos e ambientais)(...) muito diferente, é articular o risco com dimensões psicológicas e ideológicas de forma a poder falar-se do risco existencial causado pelo outro("o inimigo" o da outra "tribo" política, religiosa ou ideológica)e legitimadora do recurso a ações preventivas e repressivas constitucionalmente legitimadas e instrumentalmente concretizadas por um "direito penal do risco".* CANOTILHO, José Joaquim Gomes (2006) "Justiça Constitucional e Justiça Penal", *in Revista Brasileira de Ciências Criminais*, nº 58, São Paulo, pp. 337-338.

201 Procurando evitar alguma permissividade anterior, projectada por interpretações pródigas em encontrar *loopholes* na lei, bem como a tentação do *forum shopping*, e acolhendo conclusões do *Acórdão no Processo C-131/12 Google Spain SL, Google Inc. VS Agencia Española de Protección de Datos e Mario Costeja González*, de 13 de Maio de 2014.

202 Artigo 3.º, n.º1, do RGPD.

que não estabelecidas na União[203]*,* ofereçam bens e serviços[204] e/ou procedam ao *controlo do seu comportamento*[205]*, desde que esse comportamento tenha lugar na União*[206]. Notamos, ainda, a extensão além-fronteiras do âmbito de aplicação territorial do RGPD. Este aplica-se ainda em todos os casos em que *o tratamento de dados pessoais seja feito por um responsável pelo tratamento estabelecido fora do espaço da União*[207]*, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público*[208].

5.2. DA CLARIFICAÇÃO CONCEPTUAL: EM ESPECIAL, OS CONCEITOS DE DADOS PESSOAIS, TRATAMENTO DE DADOS PESSOAIS E CONSENTIMENTO

A *incompletude*, pela natureza naturalmente aberta com que a DPD procedeu ao elenco de definições em 1995, apresenta no RGPD uma caracterização mais consentânea com os

203 Artigo 3.º, n.º2, do RGPD.
204 Artigo 3.º, n.º2, alínea a), do RGPD.
205 Artigo 3.º, n.º2, alínea b), do RGPD.
206 Seguramente, procurando tentar mitigar as múltiplas reacções derivadas das revelações do caso *Snowden*. *Vide*, a este propósito, as afirmações de *ALAN RUSBRIDGER,* no artigo de opinião, *SOBRE A FUGA DE SNOWDEN E DE TODOS NÓS*: « (…) *Começámos a ter uma ideia de como tudo se passa. A NSA e a sua congénere britânica, o GCHQ (Government Communication Headquarters), trabalham de perto com serviços de Internet e empresas de telecomunicações para reunir enormes quantidades de dados sobre nós. Uma parte desse trabalho faz-se de forma aberta – através de pedidos legais formais. Outra parte é feita a montante das empresas de tecnologia e de telefones – ou seja, interceptando os sinais em movimento. (...).*
À medida que as revelações de Snowden continuavam, tornou-se evidente o quanto os serviços de segurança dependem da ajuda, oficial e não oficial, dos serviços comerciais que todos nós usamos – os operadores de Internet, as companhias de telefone e redes sociais. Tanto nos Estados Unidos como no Reino Unido, a bolha de secretismo legal que rodeia esta actividade é tal que nenhuma empresa ousa vir a público discutir as suas relações com os serviços secretos. É ilegal fazê-lo. Pelo que lhes toca, os Governos dos dois lados do Atlântico têm pânico que as empresas comerciais fujam caso os consumidores saibam o que têm feito com as suas informações.
Mas tive um encontro interessante (e que se manteve anónimo, claro) com alguém num cargo muito elevado numa megaempresa da costa Leste [dos EUA] que reconheceu que nem ele nem o CEO da sua organização tinham acesso às informações sobre que tipo de acordos a sua companhia fez com o Governo americano. "Então, é como uma empresa dentro da empresa?"». Publicado posteriormente no jornal Público *online*, e disponível em: https://www.publico.pt/mundo/noticia/sobre-a-fuga-de-snowden-e-todos-nos-1616896. – Último acesso Set.2016.
207 Pensamos, por exemplo, no diferendo das consequências do caso *Brexit,* e das mensagens políticas vindas da Escócia e da Irlanda. Efectivando-se a saída do Reino Unido da União, qual será o regime que vigorará na Escócia, atentas as declarações de Nicola Sturgeon «*EU WHAT? Nicola Sturgeon wants Scotland to stay in European single market even if rest of UK leaves*». Disponível em: https://www.thesun.co.uk/news/1986394/nicola-sturgeon-wants-scotland-to-stay-in-european-single-market-even-if-rest-of-uk-leaves/. – Último acesso Out.2016
208 Artigo 3.º, n.º 3, do RGPD.

desafios presentes, propostos quer pelas disciplinas do direito quer das tecnológicas. Assim, não é de todo despiciendo notar a autonomização de certos conceitos, como os de «*Limitação do tratamento*[209]»; «*Definição de perfis*[210]»; «*Pseudonimização*[211]»; «*Violação de dados pessoais*[212]»; «*Dados genéticos*[213]»; «*Dados biométricos*[214]»; «*Dados relativos à saúde*[215]»; «*Estabelecimento principal*[216]»; «*Empresa*[217]»; «*Grupo empresarial*[218]»; «*Regras vinculativas aplicáveis às empresas*[219]»; «*Tratamento transfronteiriço*[220]»; «*Serviços da sociedade da informação*[221]». Estamos na presença de conceitos definidos de forma mais aturada e que passam a fazer parte de um património léxico-jurídico comum a todo o território da União.

Pela nossa parte, cumpre-nos *autonomizar*, em especial, as *novas* definições de «*dados pessoais*[222]», «*tratamento de dados pessoais*[223]» e «*consentimento*[224]». Numa tentativa de concentrar a dispersão abstracta que estes conceitos representa(ra)m na DPD, o RGPD passa a caracterizá-los de forma exaustiva. No que diz respeito à definição de **dados pessoais**, esta é alargada, visando prevenir[225] novas formas de intrusão na esfera

209 Artigo 4.º, n.º3, do RGPD. Pense-se, por exemplo, neste caso, em "*selos temporais*".
210 Artigo 4.º, n.º4, do RGPD. Ainda que *avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever* acções passadas, presentes ou futuras, relacionadas com o seu *desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses*, entre outras, nos suscitem as maiores interjeições.
211 Artigo 4.º, n.º5, do RGPD. Vide Considerando (29):« *A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento ea conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento.*».
212 Artigo 4.º, n.º12, do RGPD.
213 Artigo 4.º, n.º13, do RGPD.
214 Artigo 4.º, n.º14, do RGPD.
215 Artigo 4.º, n.º15, do RGPD.
216 Artigo 4.º, n.º16, do RGPD.
217 Artigo 4.º, n.º18, do RGPD.
218 Artigo 4.º, n.º19, do RGPD.
219 Artigo 4.º, n.º20, do RGPD.
220 Artigo 4.º, n.º23, do RGPD.
221 Artigo 4.º, n.º25, do RGPD.
222 Artigo 4.º, n.º1, do RGPD.
223 Artigo 4.º, n.º2, do RGPD.
224 Artigo 4.º, n.º11, do RGPD.
225 *Vide*, a propósito, o Considerando (30) «*As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência (RFID). Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares*.».

protectiva dos direitos fundamentais da pessoa, no sentido de constituir instrumentos de defesa mais efectivos do direito à identidade informacional do seu titular. Em conformidade, a definição de dados pessoais passa a compreender também *identificadores* como endereços de IP[226], dados de localização e identificadores por via electrónica.

Relativamente ao conceito de **tratamento de dados**, este, precavendo uma realidade tecnológica mais *inolvidável*, pressuposta de antemão no paradigma da digitalização da sociedade e das emergentes possibilidades e riscos daí decorrentes, passa a projectar no seu leque detalhado (não exaustivo) de conceitos, o de *estruturação; recuperação; divulgação por transmissão; forma de disponibilização; limitação*. Se na definição sucedida "*tratamento*" implicava a expressão «*comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão*[227]», o RGPD passa a prescrever «*a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização*», autonomizando as técnicas de «*comparação ou*

226 Com efeito, atente-se na recente jurisprudência do TJUE, no *Processo C‑582/14, Patrick Breyer contra Bundesrepublik Deutschland.* Tratando-se, efectivamente, de uma questão *ex novo*, saber se o endereço IP de uma pessoa poderá ser considerado como «*dado pessoal*» ante um fornecedor de conteúdos, conforme notou o Advogado-Geral Manuel Campos Sánchez Bordona «(…) *no n.° 51 do Acórdão Scarlet Extended, declarou que os endereços IP são «dados pessoais protegidos, uma vez que permitem a identificação precisa dos referidos utilizadores», mas num contexto em que a recolha e identificação dos endereços IP eram realizadas por um fornecedor de acesso à Internet, e não por um* ***fornecedor de conteúdos, como no presente caso***.». Conclusões do advogado-geral, disponíveis em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d576ea2a2d8398461380f2a70eb642a9fa.e34KaxiLc3qMb40Rch0SaxyKaxr0?text=&docid=178241&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=767592#Footnote4 . – Último acesso Set.2016.
O TJUE, acolhendo em parte as conclusões propostas pelo Advogado-Geral, pronunciou-se no sentido de considerar: *« (i) O artigo 2.º, alínea a), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que um endereço de protocolo Internet dinâmico registado por um prestador de serviços de meios de comunicação em linha aquando da consulta por uma pessoa de um sítio Internet que esse prestador disponibiliza ao público constitui, relativamente a esse prestador, um dado pessoal na aceção dessa disposição, quando este disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares que o fornecedor de acesso à Internet dessa pessoa dispõe.; e, (ii) O artigo 7.º, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que se opõe a uma regulamentação de um Estado‑Membro nos termos da qual um prestador de serviços de meios de comunicação em linha apenas pode recolher e utilizar dados pessoais de um utilizador desses serviços sem o consentimento deste na medida em que essa recolha e essa utilização sejam necessárias para permitir e faturar a utilização concreta dos referidos serviços por esse utilizador, sem que o objetivo de garantir o funcionamento geral desses mesmos serviços possa justificar a utilização dos referidos dados após o termo de uma sessão de consulta desses meios de comunicação.*». Disponível em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d530a6cde8db214b85a14decac6d06c408.e34KaxiLc3qMb40Rch0SaxyKaxr0?text=&docid=184668&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=801215. – Último acesso Out.2016.
227 Artigo 2.º, alínea b), da DPD.

interconexão» desse segmento, invectivando, aqui, as definições de perfil derivadas da pegada digital que a pessoa vai, *ao de leve*, deixando na rede. Assinala-se que a tónica passa, neste aspecto em concreto, a incidir sobre a "*divulgação*" e "*forma de disponibilização*"[228], superando as limitações decorrentes da fórmula sucedida de "comunicação" e "colocação à disposição", no tocante à protecção das pessoas e dos seus dados.

Por fim, o **consentimento**. A fórmula *perversa* (que já demos conta previamente) constante da DPD[229], em que o consentimento bastava-se com uma «***qualquer*** *manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento*», foi, finalmente deposta. Regiamente, o pronome indefinido "qualquer" sucumbe na redacção do RGPD. Em acréscimo, a nova lei passa a exigir ***uma manifestação de vontade, livre, específica, informada e explícita, mediante declaração ou acto positivo inequívoco***[230] de aceitação do tratamento dos dados pessoais que lhe digam respeito por parte do seu titular. Sendo o tratamento baseado no consentimento, sempre que a isso seja instado, o responsável pelo tratamento passa a ter o ónus de demonstração desta condição[231] para que o tratamento seja considerado lícito. Com relativa bonomia, *o consentimento deve*

228 Acolhendo a clarificação operada pela interpretação do TJUE, desde logo, no Acórdão *Lindqvist*, que procedeu ao esclarecimento do (i) regime de tratamento de dados enquanto actividade pessoal ou doméstica: «*A operação que consiste na referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui um «tratamento de dados pessoais por meios total ou parcialmente automatizados»*»; (ii) a noção de transferência de dados para países terceiros: «*Não existe uma «transferência para um país terceiro de dados» na acepção do artigo 25.° da Directiva 95/46 quando uma pessoa que se encontra num Estado-Membro insere numa página Internet, de uma pessoa singular ou colectiva que alberga o sítio Internet no qual a página pode ser consultada e que está estabelecida nesse mesmo Estado ou noutro Estado-Membro, dados de carácter pessoal, tornando-os deste modo acessíveis a qualquer pessoa que se ligue à Internet, incluindo pessoas que se encontram em países terceiros*»; bem como (iii) a superação da ambiguidade derivada da transposição do quadro legal da DPD, «*…as disposições da Directiva 95/46 não contêm, em si mesmas, uma restrição contrária ao princípio geral da liberdade de expressão ou a outros direitos e liberdades que vigoram na União Europeia (...) Compete às autoridades e aos órgãos jurisdicionais nacionais encarregados de aplicar a regulamentação nacional que procede à transposição da Directiva 95/46 assegurar um justo equilíbrio entre os direitos e interesses em causa, incluindo os direitos fundamentais protegidos pela ordem jurídica comunitária*». Disponível em: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30dd28296b2724ac4b0895cf91c3f2a490df.e34KaxiLc3qMb40Rch0SaxuSaxb0?docid=48382&pageIndex=0&doclang=PT&dir=&occ=first&part=1&cid=161864 . – Último acesso Set.2016.

229 Artigo 2.º, alínea h), da DPD.

230 Vide Considerando (32): «*O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral.*»,

231 Artigo 7.º, n.º1, do RGPD.

poder ser tão fácil de retirar quanto de dar[232], até porque o titular dos dados viu positivado *o direito de retirar o seu consentimento a qualquer momento.* Finalmente, no sentido de se evitarem presunções de consentimento *ad voluntatem,* naqueles casos em que o mesmo *seja dado no contexto de uma declaração escrita que diga também respeito a outros assuntos*, o RGPD passa a exigir que o pedido de consentimento seja *apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples*, invalidando-o sempre que estas condições não sejam verificadas[233]. É pois evidente que, funcionando como causa legitimadora para o tratamento[234], o consentimento fosse outorgado como condição decisiva[235] do princípio da licitude[236] do tratamento[237].

Asseveradas, sumariamente, as *novas interconexões* que dados pessoais, tratamento e consentimento reflectem, observamos a preocupação de salvaguarda da pessoa (e dos seus dados) relativamente a múltiplas formas e técnicas de recolha, tratamento, armazenamento e conservação e disponibilização dos dados pessoais, quanto a situações que, no futuro, combinadas, poderão constituir lesões efectivas de direitos, liberdades e garantias fundamentais do seu titular. Manifesta-se a deslocação positiva, objectivando o controlo dos dados pessoais por parte dos seus titulares, alicerçando bases para o exercício

232 Artigo 7.º, n.º3, do RGPD.
233 Artigo 7.º, n.º2, do RGPD.
234 *Vide,* a propósito, a condição anteposta de invalidade (presunção) sempre que a outra parte esteja investida de funções de autoridade pública, por exemplo. *«Considerando (43)* ***A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa.*** *Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.».*
235 Decisivo, de facto. Veja-se, a título de exemplo, a recente decisão tomada pelo Comissário de Protecção de dados e de liberdade de informação alemão, *Johannes Caspar*, relativamente à partilha de dados pessoais que a empresa *Facebook* fez migrar para as suas bases de dados, da sua participada *Whatsapp.* Sem consentimento e sem base legal para esta acção, o Comissário *Caspar* ordenou a cessação imediata desta partilha, bem como a destruição dos dados pessoais, entretanto, já transmitidos. «***This administrative order protects the data of about 35 million WhatsApp users in Germany. It has to be their decision, whether they want to connect their account with Facebook. Therefore, Facebook has to ask for their permission in advance. This has not happened***.», pode ler-se no comunicado de imprensa disponibilizado. Disponível em: https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf. – Último acesso Out.2016
236 *Vide* «*Considerando (40) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa*, (…)».
237 Artigo 6.º, n.º1, alínea a), do RGPD.

de outros direitos, como por exemplo o *direito ao esquecimento*. Sob outro prisma, notamos a inquietação com o mapeamento e *profiling* derivados de dados pessoais recolhidos, tratados e a disponibilizar (sob *arquitecturas* distintas) com o decurso do tempo.

5.3. DA RETOMA DO MODELO PRINCIPIOLÓGICO PELO RGPD

O modelo do RGPD apresenta melhorias notórias em relação ao anterior modelo, em termos de clarificação conceptual e de sistematização principiológica, não obstante retome o modelo adoptado pela DPD. Na temática dos dados pessoais, estes implicam directamente um conjunto de princípios que fundamentam o seu tratamento:

5.3.1. O **princípio de licitude, lealdade e transparência**[238] - *O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados*[239]. Convocando um, inerente, princípio da responsabilidade a quem efectuar o tratamento dos dados pessoais, demanda ainda *que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado*[240].

5.3.2. O **princípio da finalidade -** Operativo, basilar, marca, indelevelmente, a temática. Concretizando o princípio anterior[241], conciso, a «*limitação das finalidades*»[242] reverbera a necessidade de que as finalidades específicas do tratamento dos dados

238 Artigo 5.º, n.º1, alínea a), do RGPD. (os dados pessoais são) «*Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados*».
239 Considerando (39) do RGPD.
240 Considerando (58) do RGPD.
241 *Vide «Considerando (60) Os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades.»*
242 Artigo 5.º, n.º1, alínea b), do RGPD. (Os dados pessoais são) «*Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1)*».

pessoais sejam explícitas e legítimas e determinadas aquando da recolha dos dados pessoais.

Assumindo o fundamento para o tratamento dos dados pessoais, importa referenciar agora a disposição principiológica quanto à qualidade destes. Qualquer um deles aparece controvertido na cardinalidade do princípio da finalidade (o binómio, indissociável, razão+finalidade serve assim de base a qualquer modalidade de tratamento de dados):

5.3.3. Com efeito, *en passant*, o **princípio da minimização dos dados**[243] - Este, exige que os dados sejam *adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados*;

5.3.4. O **princípio da exactidão**[244] - Sempre que necessário, os dados devem ser exactos e actualizados. Ademais, na impossibilidade de verificação destas condições, *devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora*;

5.3.5. O **princípio da limitação da conservação**[245] - Objectivando a jurisprudência consolidada do TJUE[246], este princípio postula que os dados deverão ser *conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados*. Admitindo excepções quanto à conservação dos dados pessoais por períodos mais longos, sempre que verifiquem as condições de tratamento *exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, número 1*, encarrega ainda o responsável pelo tratamento de *fixar os prazos para o apagamento ou a revisão periódica*[247], com vista à salvaguarda *dos direitos e liberdades do titular dos dados*.

243 Artigo 5.º, n.º1, alínea c), do RGPD.
244 Artigo 5.º, n.º1, alínea d), do RGPD.
245 Artigo 5.º, n.º1, alínea e), do RGPD.
246 Acórdão de 8 de abril de 2014, nos processos apensos *C-293/12 e C-594/12,* respectivamente, *Digital Rights Ireland e Michael Seitlinger, Christof Tschohl* e outros, doravante, Acórdão Digital Rights Ireland: *«A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.»* - disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PT. – Último acesso Set.2016.
247 Considerando (39), parte final. «*A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica.».*

5.3.6. Por fim, o **princípio da integridade e confidencialidade**[248] - Objectivam-se tratamentos de dados que garantam a respectiva segurança[249], impondo a adopção de medidas técnicas ou organizativas adequadas[250] que garantam *a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental*.

5.4. DO REFORÇO DO PRINCÍPIO DA RESPONSABILIDADE[251] NO RGPD

Optamos por autonomizar o **princípio da responsabilidade**. Justificamos. Se considerámos *supra* os princípios postulados na DPD com relativa parcimónia, acabamos por os completar, no presente excurso, com referências concisas quanto a alguns aspectos de pormenor actualizados. Não obstante, pelo excelso cunho de deveres e obrigações[252] que o RGPD empresta ao "*responsável*" [253] pelo tratamento de dados, o princípio da responsabilidade merece este destaque. O responsável pelo tratamento de dados pessoais passa a estar obrigado a garantir *a execução das medidas que forem adequadas e eficazes bem como a ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas*[254].

248 Artigo 5.º, n.º1, alínea f), do RGPD

249 Ainda o Considerando (39), final. «*Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.*».

250 «*Artigo 32.o Segurança do tratamento*

1.Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

al b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;».

251 Artigo 5.º, n.º2, do RGPD.

252 *Vide* Considerando (74): «*Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares.».*

253 Cuja definição, em sentido lato, passa a abranger, numa equitativa repartição de responsabilidades, quer o responsável directo, quer subcontratantes quer representantes, conforme se pode retirar do Artigo 4.º, números 7, 8 e 17, e da sua conjugação com vários dos artigos dispostos no RGPD; bem como das indicações abundantes ao longo do texto legal da conjunção adversativa "ou" quando o referente é "responsável pelo tratamento" (""ou" subcontratante").

254 Considerando (75) do RGPD.

Perspectivando o Mercado Único digital para a Europa[255], há, efectivamente, ao longo de todo o RGPD, uma acentuação desta vertente sobre os responsáveis, subcontratantes, representantes, no e pelo tratamento de dados pessoais, por forma a que a sensação de insegurança - por parte dos titulares dos dados pessoais - por um lado, e desresponsabilização - por parte dos "responsáveis" pelo tratamento - por outro, sejam menorizadas.

Com efeito, os deveres do responsável pelo tratamento, estendem-se desde:

(i) Uma clara e *efectiva repartição de responsabilidades*[256] entre todos os "responsáveis"[257];

(ii) Uma exigência de aplicação de técnicas e medidas organizativas[258], pressupostas num conjunto de regras específicas, como pseudonimização; cifragem; capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência em permanência dos sistemas e dos serviços de tratamento de dados; capacidades redundantes para garantir a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de um incidente físico ou técnico[259];

(iii) A uma definição de políticas adequadas em matéria de protecção de dados[260], pressupostas no dever anterior e desde que em observância ao princípio da

255 *Vide* Considerando (13): «*A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros*(…)».

256 *Vide* a propósito Considerando (79) «*A defesa dos direitos e liberdades dos titulares dos dados, bem como a responsabilidade dos responsáveis pelo seu tratamento e dos subcontratantes, incluindo no que diz respeito à supervisão e às medidas adotadas pelas autoridades de controlo, exigem uma clara repartição das responsabilidades nos termos do presente regulamento*(…)».

257 Artigos 26.º e seguintes do RPDP.

258 Artigo 24.º, número 1, do RGPD.

259 Aliás, a preocupação com a segurança dos dados das pessoas é objecto de escrutínio aturado no RGPD. Além da imposição de medidas de segurança no tratamento (artigo 32.º), é ainda imperativa a comunicação de uma violação de dados pessoais à autoridade de controlo nacional principal (Artigo 33.º), bem como a comunicação à pessoa titular dos dados, sempre que tal seja susceptível de implicar um elevado risco para os seus direitos e liberdades fundamentais.

260 Artigo 24.º, n.º2, do RGPD.

proporcionalidade, permitindo arquitecturar mecanismos de protecção de dados desde a concepção e por defeito[261];

(iv) À promoção de regras de *compliance*[262] internas e de certificação[263], as quais, em última instância, obrigarão as organizações a certificarem-se a nível da ISO27001, em sede da segurança da informação;

Em acréscimo, compete ainda ao responsável a elaboração de *avaliações de impacto sobre a protecção de dados, quando o uso de novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for susceptível de implicar um elevado risco*[264] para os direitos e liberdades fundamentais das pessoas titulares dos dados pessoais a tratar[265]. Ademais, nestes casos, passa a ser obrigatória uma consulta prévia[266] à autoridade de controlo antes do tratamento destes mesmos dados, sendo ainda obrigatório o registo de todas as actividades de tratamento[267], a cargo do responsável pelo tratamento[268]. Fica ainda plasmado um dever de cooperação institucional com a autoridade de controlo nacional[269], através da nomeação de um encarregado de protecção de dados[270] (não sendo matéria nova no contexto do quadro legal europeu[271]). Trata-se, a nosso ver, de um corolário necessário de efectivação de todo este complexo edifício

261 Artigo 25.º, do RGPD.
262 Artigo 40.º, do RGPD.
263 Artigo 42.º, do RGPD.
264 *Vide* Considerando (89):« *A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades(...).*».
265 Artigo 35.º, do RGPD.
266 Artigo 36.º, n.º2, do RGPD.
267 Exceptuando-se os casos previstos no n.º5, do artigo 30.º, do RGPD.
268 Artigo 30.º, do RGPD.
269 Artigo 31.º, do RGPD.
270 Artigo 37.º, do RGPD.
271 Vide, por exemplo o artigo 24.º, n.º8, do REGULAMENTO (CE) N.o 45/2001 DO PARLAMENTO EUROPEU E DO CONSELHO de 18 de Dezembro de 2000 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001R0045&from=EN –último acesso Set.2016), bem como a DECISÃO DA COMISSÃO de 3 de Junho de 2008 que adopta regras de execução referentes ao responsável pela protecção de dados, nos termos do n.o 8 do artigo 24.o do Regulamento (CE) n.o 45/2001 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, que passou a executar o Regulamento aludido. (disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:193:0007:0011:PT:PDF. – Último acesso Set.2016).

desenhado em torno de um tratamento e uma protecção dos dados das pessoas, consentâneas como o novo quadro regulamentar europeu. Com efeito, até pela posição que ocupará na organização em que se inserir, quer interna[272], quer externamente[273], o encarregado de protecção de dados *passa a desempenhar* uma função de especial sensibilidade no tocante à protecção dos dados das pessoas singulares.

Afigura-se-nos, enfim, que todo o conjunto enunciativo de deveres e obrigações dos "*responsáveis*", acaba por, a coberto de um regime sancionatório assaz coercitivo[274], consolidar a necessidade de um (re)equilíbrio da relação de forças. Além disso, discorrendo o novo quadro jurídico, sublinhamos este (re)centrar do ponto de partida, visando uma optimização do potencial de crescimento da economia digital[275], por um lado, bem como uma eficaz promoção dos direitos e liberdades fundamentais das pessoas, por outro.

5.5. DAS CAUSAS DE EXCLUSÃO DA ILICITUDE DO TRATAMENTO DE DADOS NO RGPD

A imposição de múltiplos deveres e obrigações ao *responsável* pelo tratamento de dados observa, complementarmente, responsabilidades na óptica do titular dos dados pessoais. Ainda que o nível de exigência não seja comparável – nem podia sê-lo –, uma das causas de licitude no tratamento de dados assenta no consentimento[276], conceito prévia e exaustivamente caracterizado. Recuperando a fórmula da DPD, um tratamento de dados lícito é-o ainda quando decorra da lei[277] e (i) *for necessário para a execução de um contrato*[278] *no qual o titular dos dados é parte, ou para diligências pré-contratuais a*

272 *Vide* Artigo 39.º, n.º1, alíneas a) a c), do RGPD.
273 *Vide* Artigo 39.º, n.º1, alíneas d) e e), do RGPD.
274 *Vide*, a propósito, artigos 83.º e 84.º, do RGPD.
275 *Vide,* por exemplo, o Comunicado de imprensa «Mercado Único Digital para a Europa: Comissão Europeia define 16 iniciativas para a sua concretização», disponível em: http://europa.eu/rapid/press-release_IP-15-4919_pt.htm . – Último acesso Set.2016.
276 Artigo 6.º, n.º1, alínea a), do RGPD.
277 *Vide* Considerando (40): « *Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.*».
278 *Vide* Considerando (44) « *O tratamento deverá ser considerado lícito caso seja necessário no contexto de um contrato ou da intenção de celebrar um contrato*.».

pedido do titular dos dados[279]; (ii) *for necessário para a defesa de interesses vitais*[280] *do titular dos dados ou de outra pessoa singular*[281]; (iii) *for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública*[282] *de que está investido o responsável pelo tratamento*[283]; *(iv) for necessário para o cumprimento de uma obrigação jurídica*[284] *a que o responsável pelo tratamento esteja sujeito*[285]; (v) *for necessário para efeito dos interesses legítimos*[286] *prosseguidos pelo responsável pelo tratamento ou por terceiros*[287].

Alteramos a ordem propositadamente. Relegamos a justificação dos "*interesses legítimos*" para final, porquanto a anterior ambiguidade (na DPD) do conceito indeterminado passa a demandar níveis mais exigentes de verificação. Com efeito, logo na parte final da alínea f), do número 1, do artigo 6.º, justifica-se a ilicitude dos tratamentos contrários *aos interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.* Notamos uma particular preocupação com as crianças, à qual voltaremos mais adiante. De resto, o responsável pelo tratamento, mesmo em condições de tratamento lícito, passa a ter de comprovar *os seus interesses legítimos imperiosos*[288], supostamente prevalecentes sobre

279 Artigo 6.º, n.º1, alínea b), do RGPD.
280 *Vide* Considerando (46) «*O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular.(...) Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana*.».
281 Artigo 6.º, n.º1, alínea d), do RGPD.
282 *Vide*, por exemplo, Considerando (45): «*Sempre que o tratamento dos (...) for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública, o tratamento deverá assentar no direito da União ou de um Estado-Membro.(...) Deverá igualmente caber ao direito da União ou dos Estados-Membros determinar se o responsável pelo tratamento que exerce funções de interesse público ou prerrogativas de autoridade pública deverá ser uma autoridade pública ou outra pessoa singular ou coletiva de direito público, ou, caso tal seja do interesse público, incluindo por motivos de saúde, como motivos de saúde pública e proteção social e de gestão dos serviços de saúde, de direito privado, por exemplo uma associação profissional.».*
283 Artigo 6.º, n.º1, alínea e), do RGPD.
284 Veja-se, novamente, o Considerando (45).
285 Artigo 6.º, n.º1, alínea c), do RGPD.
286 *Vide* Considerando (47) «*Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável.».*
287 Artigo 6.º, n.º1, alínea f), do RGPD.
288 *Vide* Considerando (69). «No caso de um tratamento de dados pessoais lícito realizado(…)por motivos de interesse legítimo do responsável pelo tratamento ou de terceiros(…)cabe(r) ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados.

os interesses ou direitos e liberdades fundamentais do titular dos dados. Se o consentimento tácito[289] deixa de se presumir válido, é agora, também, necessário que o responsável pelo tratamento *demonstre que o titular deu o seu consentimento à operação de tratamento dos dados*[290]. Convoca-nos, por fim, algum embaraço que *um tratamento que seja tido como necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento* não seja lícito *quando o tratamento for efectuado por autoridades públicas na prossecução das suas atribuições por via eletrónica*[291]. Porém, admitimos a sua inserção.

Concedemos, de antemão, a margem de liberdade concedida pelo legislador europeu aos legisladores nacionais de cada E.M. Obviamente. O RGPD confere alguma margem decisória aos legisladores nacionais para *manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras*, *nos casos que envolvam cumprimento de uma obrigação jurídica,* ou, *nos casos que se mostre necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública*, desde que esta concentre a definição legislativa de forma mais precisa, garantindo sempre a licitude e lealdade do tratamento[292].

---

289 *Vide* (ainda) o Considerando (32) « (…) *O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento.».*

290 Vide Considerando (42): «*Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance.*».

291 A aposição deste complemento à alínea f) permite-nos, por exemplo, convocar a seguinte questão. O considerando (47), parte final, «(…)*Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento.*». Ora, a aparente *contradictio in terminis* entre o considerando e a letra da lei, desloca-nos para punção da realidade portuguesa. Poderemos alvitrar que quando o tratamento é efectuado por autoridades públicas na prossecução das suas atribuições por via eletrónica, o RGPD não é aplicável?

Se o combate à fraude, como julga o Considerando, pode ser interpretado como um interesse legítimo, porque razão o RGPD não objectivou a sua materialização na letra da lei? Evitar-se-iam interpretações *sui generis* por cada EM, por exemplo. No caso português, em particular, estamos a pensar nos casos mediáticos envolvendo *listas vip* e a autoridade tributária. Ou na intenção recente de permitir um acesso – quase indiscriminado - por parte da autoridade tributária às contas dos cidadãos. Afastando-se o RGPD, a uniformização que se pretende(ria) com o RGPD demite-se, *ingloriamente*, do arremesso argumentativo nos processos judiciais?

Seja como for, a CRP não se demite deste exercício jurídico. Atente-se por exemplo, na interpretação constitucional feita pela CNPD, que acompanhamos, a propósito da intenção do governo em conceder acesso automático à AT às contas dos residentes em território português.

O Parecer n.º22/2016, de 05 de Julho, poderá ser consultado em: https://www.cnpd.pt/bin/decisoes/Par/40_22_2016.pdf . – Último acesso Out.2016.

292 Artigo 6.º, n.º2, do RGPD.

Sublinhe-se, ainda, que, nos casos em que o tratamento seja feito *para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos, não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros*[293], para que o tratamento seja lícito é, agora, necessário que o responsável pelo tratamento para outros fins afira da sua compatibilidade com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, e o conjugue com (i) *a finalidade do tratamento posterior*[294]*;* (ii) *o contexto em que os dados pessoais foram recolhidos*[295]; (iii) *a natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais foram tratadas*[296]; (iv) *as eventuais consequências do tratamento posterior pretendido para os titulares*[297]; e, (v) *a existência de salvaguardas adequadas, como a cifragem ou a pseudonimização*[298].

Por fim, afirmamos, despudoradamente, que a sistematização dos direitos inerentes aos titulares dos dados pessoais, positivada no RGPD, se afigura de compreensão *inteligível*. De facto, o titular dos dados, para poder exercer qualquer tipo de direito de que usufrui em tratamentos de dados que lhe digam respeito, terá forçosamente de compreender a estrutura destes mecanismos de defesa, *de forma concisa, transparente, inteligível e de fácil acesso, suportada numa linguagem clara e simples*. É justamente nestes termos que o RGPD reclama a transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares dos dados[299]. O responsável pelo tratamento deve *facilitar o exercício dos direitos do titular dos dados nos termos dos artigos 15.º a 22.º* [300], elencando, consecutivamente, um conjunto de regras a observar por parte do(s) responsáveis pelo tratamento de dados pessoais, das quais destacaríamos a tempestividade das reacções em função de solicitações de índole variada de pedidos de informação por parte do titular dos dados. Concedendo, por regra, a gratuitidade[301] da disponibilização de informação a facultar ao titular dos dados, *curiosamente*, aventando

293 Artigo 6.º, n.º4, do RGPD.
294 Artigo 6.º, n.º 4, alínea a), do RGPD.
295 Artigo 6.º, n.º 4, alínea b), do RGPD.
296 Artigo 6.º, n.º 4, alínea c), do RGPD.
297 Artigo 6.º, n.º 4, alínea d), do RGPD.
298 Artigo 6.º, n.º 4, alínea e), do RGPD.
299 Artigo 12.º, do RGPD.
300 Artigo 12.º, n.º 2, do RGPD.
301 Art.º 12.º, n.º5, 1.ª parte: «As informações fornecidas nos termos dos artigos 13.º e 14.º e quaisquer comunicações e medidas tomadas nos termos dos artigos 15.º a 22.º e 34.º são fornecidas a título gratuito.»

a putativa paranoide repetividade de pedidos idênticos, o RGPD consente que o responsável pelo tratamento possa: (i) *Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas*[302]; (ii) *Recusar-se a dar seguimento ao pedido*[303]; ainda que o ónus da demonstração do carácter manifestamente infundado ou excessivo dos pedidos fique a cargo deste[304].

5.6. DO ELENCO GARANTÍSTICO DO RGPD: NOVOS DIREITOS, DIREITOS MAIS ROBUSTOS E COM MENOS LIMITAÇÕES

Concentremo-nos, nas próximas páginas da presente dissertação, no elenco dos direitos expressamente positivados no RGPD. Pela nossa parte, parece-nos claramente que o novo Regulamento alarga a lista de direitos dos titulares dos dados, ora prevendo, *ex novo*, novas posições jurídicas de vantagem, ora enrobustecendo as herdadas da DPD. Em acréscimo, foi reduzido o elenco das limitações ao exercício desses mesmos direitos.

5.6.1. A temática dos direitos e do seu exercício, no RGPD, *concentra-se*, no essencial, em torno das disposições entre os artigos 15.º e 22.º. Apresentando-se sistematizados em secções específicas, encontram-se, porém, apenas limitados no exercício, pelas condições vertidas no artigo 23.º. Por força do direito da União ou do E.M. em causa, ao qual o responsável pelo tratamento esteja sujeito, a lei, desde que a limitação respeite a essência dos direitos fundamentais e se constitua como medida necessária e proporcional, poderá *limitar o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º*, sempre que esteja em causa assegurar: *(a) A segurança do Estado; (b) A defesa; (c) A segurança pública; (d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais; (e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro; (f) A defesa da independência judiciária e dos processos judiciais; (g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas; (h) Uma missão de controlo, de inspeção ou de regulamentação*

302 Artigo 12.º, n.º 5, alínea a), do RGPD.
303 Artigo 12.º, n.º 5, alínea b), do RGPD.
304 Artigo 12.º, n.º 5, alínea b), parágrafo segundo, do RGPD.

associada, ainda que ocasionalmente, ao exercício da autoridade pública; (i) A defesa do titular dos dados ou dos direitos e liberdades de outrem; (j) A execução de ações cíveis[305].

5.6.2. No que se refere aos direitos propriamente ditos cabe, em primeiro lugar, destacar o **direito à informação**. A sistematização a que aludimos reflecte os deveres e obrigações dos responsáveis pelo tratamento de dados. Neste conspecto, distinguindo a forma de recolha dos dados pessoais (se junto do seu titular[306], se na sua ausência[307]), o RGPD postula, além do leque de informações *típicas* a disponibilizar como a identidade e contactos do responsável, ou representante[308], as finalidades e os fundamentos jurídicos para o respectivo tratamento[309]. Pela matéria nova que revela, o RGPD postula, igualmente, um *novo* leque, exaustivo, de informações a disponibilizar pelo *responsável*. Dispensando-as no caso de o titular dos dados pessoais delas já tiver conhecimento[310], temos que o responsável passa a estar obrigado a facultar informações quanto: (i) *os contactos do encarregado da proteção de dados*[311]; (ii) *os interesses legítimos do responsável pelo tratamento ou de um terceiro*[312]; (iii) *destinatários ou categorias de destinatários dos dados pessoais*[313]; e, (iv) *garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas*[314], na iminência de transferências ou até no caso de transferências já consumadas. Adensando a qualidade de informações a disponibilizar, passa a ser igualmente necessário, por forma a garantir um tratamento equitativo e transparente, o complemento de informações adicionais, vertido no número 2, deste artigo 13.º, tais como: (a) *Prazo de conservação dos dados pessoais*; (b) *a existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação,apagamento, limitação do tratamento, direito de se opor ao tratamento, bem como do direito à portabilidade dos dados*; (c) em determinadas circunstâncias, *a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado*

305 Artigo 23.º, n.º1, do RGPD.
306 Artigo 13.º, do RGPD.
307 Artigo 14.º, do RGPD.
308 Artigo 13.º, n.º1, alínea a), do RGPD.
309 Artigo 13.º, n.º1, alínea c), do RGPD.
310 Artigo 13.º, n.º4, do RGPD.
311 Artigo 13.º, n.º1, alínea b), do RGPD.
312 Artigo 13.º, n.º1, alínea d), do RGPD.
313 Artigo 13.º, n.º1, alínea e), do RGPD.
314 Artigo 13.º, n.º1, alínea f), do RGPD.

com base no consentimento previamente dado; (d) *o direito de apresentar reclamação a uma autoridade de controlo*; (e) *se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato*; (f) *a existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados*. Adicionalmente, nos casos em que o responsável pelo tratamento *tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes*[315], de que o titular necessite ter conhecimento.

Na ausência do seu titular no momento da recolha dos dados[316], não diferindo muito no amplo espectro outorgado no artigo anterior, passa a ser também obrigatório para o responsável pelo tratamento dos dados pessoais, informar o titular dos dados quanto à origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público[317]. O conjunto das informações a disponibilizar impõem, neste caso, pela ausência do seu titular no acto da recolha, a obrigação de comunicação, por parte do *responsável*: (i) *num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados*[318]; (ii) nos casos em que os dados se destinem a ser utilizados *para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação*[319]; e, (iii) nos casos em que possa estar prevista *a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados*[320]. Concomitantemente, o RGPD dispensa a aplicação deste leque de informações, nos termos do número 5, do artigo 14.º, sempre que (b) *se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, investigação científica ou histórica ou estatísticos*; (c) *a obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou*

315 Artigo 13.º, n.º3, do RGPD.
316 Artigo 14.º, do RGPD.
317 Artigo 14.º, n.º2, alínea), do RGPD.
318 Artigo 14.º, n.º3, alínea a), do RGPD
319 Artigo 14.º, n.º3, alínea b), do RGPD
320 Artigo 14.º, n.º3, alínea c), do RGPD

do Estado-Membro, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; (d) *os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro.* Causa-nos, todavia, uma certa inquietude o enquadramento da dispensa de informar prevista na alínea, *in casu*, *a) o titular dos dados já tenha conhecimento das informações*. Pensamos nas condições de efectividade desta disposição. Assumindo que os dados foram recolhidos na ausência do seu titular, qual foi a forma usada para que ele disso tivesse conhecimento? Interposta pessoa? Notícia de jornal[321]? Qualquer uma destas hipóteses é condição suficiente para efectivar *a dispensa de informar*?

Nuclear, paralela e complementarmente ao direito à informação, com o qual partilha aliás a Secção II onde se inserem, cumpre destacar o **direito de acesso**[322]. A pessoa titular dos dados, usufruindo do direito de confirmação sobre o objecto do tratamento de dados que lhe digam respeito, tem o direito de aceder quer aos seus dados pessoais quer às informações como: *(i) finalidades; (ii) categorias dos dados pessoais (iii) destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados; (iv) o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; (v) o direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos seus dados pessoais, ou do direito de se opor a esse tratamento; (vi) o direito de apresentar reclamação a uma autoridade de controlo; (vii) quando os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; (viii) a existência de decisões automatizadas, incluindo a definição de perfis*.

E ainda, o **direito de rectificação**[323]. Permite que a pessoa titular dos dados possa demandar, sem demora injustificada, o responsável pelo tratamento dos dados, com vista à correcção dos dados que lhe dizendo respeito, caso se mostrem inexactos. Apurada a finalidade do tratamento, se tal for necessário, o direito a que os dados pessoais incompletos possam ser completados, poderá constituir-se por via de uma declaração adicional.

---

321 *Base de dados com emails de portugueses à venda na Internet por 40 euros*. Notícia disponível em: http://www.jornaleconomico.sapo.pt/noticias/base-dados-emails-portugueses-venda-na-internet-40-euros-83960#.WBTdqC0rLIU – Último acesso Out.2016.
322 Artigo 15.º, do RGPD.
323 Artigo 16.º, do RGPD.

5.6.3. Novidades no RGPD são, neste particular, o direito de portabilidade dos dados[324], o direito à limitação do tratamento[325] e o direito ao apagamento dos dados ("*direito a ser esquecido*")[326].

5.6.3.1. O **direito de portabilidade dos dados**, por norma, verificadas cumulativamente as condições das alíneas a) e b), do número 1, do Artigo 20.º, conferem à pessoa titular dos dados pessoais que lhe digam respeito o direito de os receber e de os transmitir a outro responsável pelo tratamento, sem que o responsável inicial a tal se possa opor. No exercício deste direito, e sem prejuízo dos direitos e liberdades de terceiros[327], sempre que as condições técnicas o permitam, o titular dos dados tem ainda *o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento*[328].

5.6.3.2. Por sua vez, quanto ao **direito à limitação do tratamento**, este postula uma condição de suspensão do tratamento de dados, sempre que se verifiquem as situações previstas nas alíneas a) a d), do número 1, do artigo 18.º[329]. Sempre que a suspensão do tratamento dos dados pessoais se verifique, à excepção da conservação, os dados pessoais só poderão ser objecto de tratamento se a pessoa deles titular tiver *dado consentimento, se for necessário para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro*[330].

5.6.4. Finalmente, o **direito ao apagamento dos dados**. A formulação e positivação deste *direito a ser esquecido*, deriva, em grande medida, da jurisprudência do TJUE[331]. Sendo

---

324 Artigo 20.º, do RGPD.
325 Artigo 18.º, do RGPD.
326 Artigo 17.º, do RGPD.
327 Artigo 20.º, n.º4, do RGPD.
328 Artigo 20.º, n.º2, do RGPD.
329 «a) O *titular contesta a exactidão dos seus dados durante um período que permite ao responsável verificar a sua exatidão*; b) *no âmbito de um tratamento ilícito, o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização*, salvando os efeitos (alguns) do tratamento inicial; c) *o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial*; d) o titular tiver exercido o seu direito de oposição, *até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados*.»,
330 Artigo 18.º, n.º2, do RGPD.
331 *Google Spain SL, Google Inc. VS Agencia Española de Protección de Datos e Mario Costeja González (Processo C-131/12) de 13 de Maio de 2014.* Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=4984

certo que aprofundaremos posteriormente este direito (até porque do seu correcto desenho poder-se-á estabilizar o direito à identidade informacional que perscrutamos e sobre o qual discorre grande parte da presente investigação), compete-nos, porém, adiantar alguns dos aspectos mais relevantes vertidos na letra da lei. Pensemos, a propósito, na temática dos dados pessoais, das zonas conflituantes que o direito ao apagamento dos dados poderá trilhar. Entre outros, este direito poderá apresentar-se em confronto com a *liberdade de expressão e de informação*[332]; ou com o *cumprimento de uma obrigação legal de que decorra a exigência de tratamento para o exercício de funções de interesse ou de autoridade pública*[333]; com *motivos de interesse público no domínio da saúde pública*[334]; com *fins de arquivo de interesse público, de investigação científica ou histórica ou estatísticos*[335]; ou, com *efeitos de declaração, exercício ou defesa de um direito num processo judicial*[336]. Efectivamente, estas condições correspondem àquelas que, por princípio, ponderadas em cada situação concreta, limitarão o exercício do direito ao apagamento dos dados[337].

Definida a margem de actuação, o direito a ser esquecido adquire amplitude considerável de exercício. Sem demora injustificada, quer quanto à resposta a obter quer quanto ao acto posterior a realizar, a pessoa titular dos dados pessoais tem o direito de obrigar o responsável pelo tratamento a proceder ao apagamento dos seus dados sempre que: a) *deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento*; b) *retire o consentimento em que se baseia o tratamento* e não exista outro fundamento jurídico para o referido tratamento; c) exerça o seu direito de oposição e este prevaleça sobre interesses legítimos que justificassem o tratamento, ou quando tenha exercido o seu direito de oposição para efeitos de *mala directa*, d) os dados tenham sido ilicitamente tratados; e) *o cumprimento de obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito* assim o determine; e, f) *os dados pessoais recolhidos no contexto da sociedade da informação não respeitem* os limites legais etários ou a forma de suprimento da incapacidade jurídica do menor de 16 anos. *Novidade ainda* é que sempre que se verifiquem as condições de exercício do

332 Artigo 17.º, n.º3, alínea a), do RGPD.
333 Artigo 17.º, n.º3, alínea b), do RGPD.
334 Artigo 17.º, n.º3, alínea c), do RGPD.
335 Artigo 17.º, n.º3, alínea d), do RGPD.
336 Artigo 17.º, n.º3, alínea e), do RGPD.
337 Artigo 17.º, n.º3 do RGPD.

direito elencadas no número 1, do artigo 17.º, do RGPD, caberá ao responsável pelo tratamento dos dados, que os tiver tornado públicos, tomar as medidas razoáveis, incluindo de carácter técnico, atento o estado da arte e os custos dessas medidas, *para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos*[338].

5.6.5. Notas finais para o **direito de oposição**[339] e as **decisões individuais automatizadas,** incluindo definição de perfis[340]. Caracterizando a Secção IV do Capítulo dos direitos do titular dos dados, estes dois direitos complementam-se. Conferindo um direito de oposição, a qualquer momento, sempre que se a pessoa titular dos dados verifique um (i) *tratamento de dados no exercício de funções de interesse público ou ao exercício da autoridade pública*; (ii) *interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros*, (iii) *tratamento para fins diversos da finalidade com que foram recolhidos ou este não for realizado com base no consentimento*, tal não significa que a vontade da pessoa titular dos dados pessoais prevaleça. Aliás, o contexto de efectivação deste direito - a cessação do tratamento - encontra-se sujeita a uma aferição casuística, condicionado na forma por uma justificação fundada em razões imperiosas e legítimas que derrogue os interesses, direitos e liberdades da pessoa titular dos dados[341]. Impõe-se ainda através de um dever de comunicação das consequências e efeitos da manifestação de oposição, apresentado de modo claro e distinto de quaisquer outras informações[342]. Desta forma, a fórmula apresentada para o exercício do direito de oposição para efeitos de comercialização directa parece-nos mais próxima de um imperativo de controlo por parte da pessoa titular dos dados pessoais e da pegada que ela vai deixando na rede. Ademais, ao permitir que o titular se oponha a qualquer momento, e que esta oposição abranja ainda a definição de perfis relacionados com a comercialização directa, e ao obrigar que o responsável cesse o tratamento dos dados para esse fim[343], a pessoa titular dos dados arroga-se de algum controlo sobre *partes de si*, que vão sendo acumuladas por um certo *decisionismo* individual automatizado. Ainda que

338 Artigo 17.º, n.º2, do RGPD.
339 Artigo 21.º, do RGPD.
340 Artigo 22.º, do RGPD.
341 Artigo 21.º, n.º1, do RGPD.
342 Artigo 21.º, n.º4, do RGPD.
343 Artigo 21.º, n.º3, do RGPD.

este possa afastar o direito de não ficar submetido a decisões tomadas exclusivamente com base em tratamentos automatizados, sempre que se verifique (i) *a sua necessidade para a celebração ou a execução de um contrato*; (ii) *estiver autorizada pelo direito da União ou do EM*; ou, (iii) *estiver pressuposta no seu consentimento explícito*; sempre que o tratamento automatizado produza efeitos na esfera jurídica da pessoa titular dos dados ou que o afecte significativamente, a pessoa pode opor-se, sendo-lhe conferido o direito de não ficar sujeita a decisões fundadas no tratamento automatizado[344].

Condensada, em traços gerais, a disposição de princípios, garantias e direitos constante do RGPD, cumpre-nos apenas, em apelo à economia do objecto da presente investigação, sumariar algumas das novidades que acompanham o novo quadro regulatório europeu em matéria de protecção de dados.

5.7. AINDA SOBRE ALGUMAS DAS NOVAS REGRAS DO RGPD NO CONTEXTO REGULATÓRIO EUROPEU

O RGPD, enquanto instrumento regulatório uniformizador para o espaço da União, postula uma série de novidades. Se já demos conta, por exemplo, do alargamento do objecto de aplicação material além-fronteiras a entidades sediadas fora do espaço comunitário, assim como o acentuar do nível de responsabilização, sufragando um conjunto considerável de deveres e obrigações, acometido a todos os responsáveis pelo tratamento de dados pessoais, passa a ser imprescindível confirmar, por um lado, que todo este laborioso mecanismo de protecção e defesa da pessoa e dos dados pessoais, e, por outro lado, de promoção das oportunidades da economia digital e do mercado único digital para a europa, possam entrecruzar-se com relativa simplicidade e eficácia.

Encaramos, por isso, com relativa quietude o reforço das restrições quanto à transferência de dados pessoais para um país terceiro. Aliás o Capítulo V, dedicado em exclusivo a esta temática, admite como princípio geral[345] que «*Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento*.». As transferências só passam,

344 Artigo 22.º, n.º1, do RGPD.
345 Artigo 44.º, parte final, do RGPD.

por regra, o crivo da validade se o responsável pelo tratamento garantir o cumprimento das condições, entretanto, estabelecidas. O mesmo será dizer que as transferências[346] passam a ser objecto de escrutínio por parte de uma decisão de adequação[347], emitida pela Comissão[348]; ou, na sua falta, os responsáveis pelo tratamento deverão apresentar *garantias adequadas de cumprimento*[349] do RGPD ao EM ou à autoridade nacional de controlo competentes[350].

Da mesma forma, note-se o reforço da importância das autoridades nacionais de controlo. Assumem a superintendência[351] de toda a temática dos dados pessoais, enquanto *privacy watch dogs*[352], com o *fim de defender os direitos e liberdades fundamentais das pessoas*

346 Certamente, acolhendo a decisão jurisprudencial do TJUE relativamente ao *Processo C-362/14, de 6 de Outubro de 2015, Facebook Ireland/Max Schrems*, que acabou por invalidar a Decisão 2000/520, também conhecida como Acordo «Porto Seguro»(*safe harbor agreement*).
Vide, a propósito, a Conclusão 78 «*A este respeito, importa referir que, tendo em conta, por um lado, o importante papel desempenhado pela proteção de dados pessoais à luz do direito fundamental ao respeito da vida privada e, por outro, o elevado número de pessoas cujos direitos fundamentais podem ser violados em caso de transferência de dados pessoais para um país terceiro que não assegure um nível de proteção adequado, o poder de apreciação da Comissão quanto à adequação do nível de proteção assegurado por um país terceiro é reduzido, pelo que se deve proceder a uma fiscalização estrita das exigências que decorrem do artigo 25.° da Diretiva 95/46, lido à luz da Carta (v., por analogia, acórdão Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.os 47 e 48).»;* e bem assim, a Conclusão 90 do mesmo Acórdão:«(…) *aquela instituição(Comissão) concluiu que as autoridades americanas podiam aceder aos dados pessoais transferidos dos Estados-Membros para os Estados Unidos e tratá-los de um modo incompatível, nomeadamente, com as finalidades da sua transferência, para além do que era estritamente necessário e proporcionado à proteção da segurança nacional. De igual modo, a Comissão concluiu que os interessados não dispunham de vias de direito administrativas ou judiciais que lhes permitissem, nomeadamente, aceder aos dados que lhes dizem respeito e, sendo caso disso, obter a sua retificação ou supressão.».* Acórdão disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=pt#Footnote* . – Último acesso Set.2016.
347 Artigo 45.º, do RGPD.
348 Que passa a publicar no *Jornal Oficial da União Europeia e no seu sítio web uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado*. Artigo 45.º, n.º8, do RGPD.
349 *Vide* Considerando (108): «(…)*Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de proteção de dados desde a conceção e por defeito.».*
350 Artigo 46.º, do RGPD.
351 *Vide* Considerando (117): «*A criação de autoridades de controlo nos Estados-Membros, habilitadas a desempenhar as suas funções e a exercer os seus poderes com total independência, constitui um elemento essencial da proteção das pessoas singulares no que respeita ao tratamento dos seus dados pessoais*.».
352 Múltiplos factores poderão contribuir para uma *abstenção de participação na rede*. Desde a violação de dados a intromissões abusivas nas comunicações de ordem variada, mais das vezes, estes

singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União[353]. Das competências, poderes e atribuições vertidas ao longo de todo o Capítulo VI do RGPD, salientaríamos desde logo a definição de autoridade de controlo principal. Pelas múltiplas implicações que tal representa. Não *desautorizando*[354], de todo[355], as autoridades de controlo interessadas, a autoridade de controlo principal, por norma, constitui-se em função da localização do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante[356]. Uma vez definida, permite-se funcionar como *balcão único* (*one-stop-shop)*[357]. Investida do complexo de atribuições[358] e de poderes[359], e uma vez estabelecidas as regras de actividade, é precisamente na delimitação clara, numa base caso a caso, e de estreita cooperação[360] e assistência mútua[361] entre as autoridades nacionais de controlo principal e as autoridades de controlo interessadas que reside substancial parte da fundamentalidade[362] da protecção

---

condicionalismos negam a possibilidade da pessoa, receosa das consequências, de participar, revelando uma espécie de *chilling effect*. Daí que as autoridades de supervisão da protecção de dados, as autoridades nacionais de controlo, desempenhem um papel acrescido na promoção e defesa do património comum que é a fruição em liberdade e segurança desta ferramenta que nos serve que é a *internet.*

Por exemplo, o *Grupo de Trabalho do Artigo 29.º* (*Article 29 WP*), por intermédio da sua Chairwoman, Isabelle FALQUE-PIERROTIN, preocupado com violação de dados envolvendo a empresa *Yahoo,* solicitou, recentemente, informações criteriosas à sua CEO, Marissa MAYER, a propósito quer da *massiva violação de dados* que ocorreu em 2014 e que só há pouco foi dada a conhecer, quer das alegadas intromissões nos emails dos seus clientes, a coberto de solicitações das agências de inteligência americanas. Missiva disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20161027__letter_of_the_chair_of_the_art_29_wp_yahoo_en.pdf . – Último acesso Out.2016

353 Artigo 51.º, n.º1, do RGPD.

354 *Vide* Considerando (125): «*A autoridade principal deverá ser competente para adotar decisões vinculativas relativamente a medidas que deem execução às competências que lhe tenham sido atribuídas nos termos do presente regulamento. Na sua qualidade de autoridade principal, a autoridade de controlo deverá implicar no processo decisório e coordenar as autoridades de controlo interessadas. Nos casos em que a decisão consista em rejeitar no todo ou em parte a reclamação apresentada pelo titular dos dados, esta deverá ser adotada pela autoridade de controlo à qual a reclamação tenha sido apresentada.*».

355 «*Cada autoridade de controlo é competente para tratar reclamações que lhe sejam apresentadas ou a eventuais violações do presente regulamento se a matéria em apreço estiver relacionada apenas com um estabelecimento no seu Estado-Membro ou se afetar substancialmente titulares de dados apenas no seu Estado-Membro.*» Artigo 56.º, n.º2, do RGPD.

356 Artigo 56, n.º1, do RGPD.

357 «*A autoridade de controlo principal é o único interlocutor do responsável pelo tratamento ou do subcontratante no tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante.»* Artigo 56.º, n.º6 do RGPD.

358 Artigo 57.º, do RGPD.

359 Artigo 58.º, do RGPD.

360 Artigo 60.º, do RGPD.

361 Artigo 61.º, do RGPD.

362 *Vide* Considerando (127): «*As autoridades de controlo que não atuem como autoridade de controlo principal deverão ter competência para tratar casos a nível local quando o responsável pelo tratamento ou subcontratante estiver estabelecido em vários Estados-Membros (...) a autoridade de controlo deverá informar imediatamente do assunto a autoridade de controlo principal. Após ter sido informada, a autoridade de controlo principal decidirá se trata o caso de acordo com o disposto em matéria de cooperação entre a autoridade de controlo principal e a outra autoridade de controlo interessada («mecanismo de balcão único»), ou se deverá ser a autoridade de controlo que a informou a tratar o caso*

de dados pessoais. Ademais, a forte vertente fiscalizadora e um *completamente* novo e agravado quadro sancionatório[363], funcionarão como condição suficiente – assim se espera - *para controlar e executar a aplicação do RGPD*.

Notas finalíssimas apenas para destacar: (i) os *relatórios de actividade*[364] que as autoridades de controlo elaborem e que, *incluindo listagens dos tipos de violação notificadas e dos tipos de medidas tomadas em função das auditorias que realizem*, permitirão uma fiscalização acrescida – pela sua discussão pública transnacional – do estado da arte no que toca à protecção de dados[365]; (ii) o *procedimento de controlo da coerência*[366]. Particularmente, quanto a este procedimento, verifica-se que o mesmo exibe efeitos horizontais e verticais na sua execução. Se, por um lado, este procedimento reforçará os laços de cooperação e assistência mútua entre autoridades de controlo nacionais[367], e bem assim com a própria Comissão (ao nível do quadro interinstitucional europeu); por outro lado, a competência para a aprovação de regras vinculativas aplicáveis às empresas[368], por parte das autoridades nacionais de controlo, propõe-se reforçar uma aplicação mais uniforme (ao nível empresarial) do novo quadro regulamentar europeu.

---

a nível local. Ao decidir se trata o caso, a autoridade de controlo principal deverá ter em conta se há algum estabelecimento do responsável pelo tratamento ou subcontratante no Estado-Membro da autoridade de controlo que a informou, a fim de garantir a eficaz execução da decisão relativamente ao responsável pelo tratamento ou subcontratante. Quando a autoridade de controlo principal decide tratar o caso, a autoridade de controlo que a informou deverá ter a possibilidade de apresentar um projeto de decisão, que a autoridade de controlo principal deverá ter na melhor conta quando prepara o seu projeto de decisão no âmbito desse mecanismo de balcão único.».

363 *Vide* Artigos 83.º e 84.º, por exemplo, do RGPD.

364 Artigo 59.º, do RGPD.

365 Importa, ainda, salientar o Considerando (132): «*As atividades de sensibilização das autoridades de controlo dirigidas ao público deverão incluir medidas específicas a favor dos responsáveis pelo tratamento e subcontratantes, incluindo as micro, pequenas e médias empresas, bem como as pessoas singulares, em particular num contexto educacional.*»; bem como o contexto das atribuições vertido no artigo 57.º, n.º1, alíneas b) e d), do RGPD.

366 Artigo 63.º, do RGPD.

367 *Vide* Considerando (135): «*A fim de assegurar a aplicação coerente do presente regulamento em toda a União, deverá ser criado um procedimento de controlo da coerência e para a cooperação entre as autoridades de controlo. Esse procedimento deverá ser aplicável, nomeadamente, quando uma autoridade de controlo tenciona adotar uma medida que vise produzir efeitos legais em relação a operações de tratamento que afetem substancialmente um número significativo de titulares de dados em vários Estados-Membros. Deverá aplicar-se igualmente sempre que uma autoridade de controlo interessada, ou a Comissão, solicitar que essa matéria seja tratada no âmbito do procedimento de controlo da coerência. Esse procedimento não deverá prejudicar medidas que a Comissão possa tomar no exercício das suas competências nos termos dos Tratados*.».

368 Artigo 47.º, do RGPD.

Por último, se a DPD não considerava, pelo menos de forma directa, a questão da protecção dos dados dos menores (até porque, em 1995, por exemplo, o fenómeno do jogo *online Pókemon Go*[369] [370] ainda estaria a anos de luz de se concretizar), o RGPD passou a considerar a questão com relativa ponderação[371]. A vulnerabilidade intrínseca das crianças, desde logo pela sua imaturidade quanto à percepção dos riscos a que poderão estar expostas e das consequências que uma decisão sua possa acarretar - a propósito da licitude quanto ao tratamento dos seus dados pessoais e ao consentimento que lhes for dirigido –, reclama um nível de protecção específico[372], por regra de maior amplitude que o das restantes pessoas. Só desta forma se salvaguardará um natural e em liberdade exercício do seu direito ao desenvolvimento da personalidade.

Concomitantemente, é imperioso tomar sempre em consideração o superior interesse das crianças. Fulcral. Por exemplo, fruto da imaturidade que lhes é inerente, é necessário que, para um tratamento de dados lícito, este respeite as condições de aplicabilidade ínsitas no artigo 8.º, do RGPD: desde logo, um limite mínimo etário dos 16 anos ou a respectiva forma de suprimento da incapacidade jurídica do menor. De todo o modo, efectivado o tratamento de dados do menor, este, entretanto adulto, pode exercer o seu direito ao apagamento dos seus dados[373], como já demos conta previamente. Particularmente *polido*, constatar o facto de que uma das atribuições da autoridade nacional de controlo passe pela promoção de acções de formação e sensibilização, com particular atenção às

369 E bem assim, os riscos associados a uma prática regular *online* por parte dos menores era desconsiderada, algo bem diferente da realidade actual, como, por exemplo, a notícia sobre o fenómeno aludido procura evidenciar. Veja-se: http://globalnews.ca/news/2822576/pokemon-go-what-parents-should-know-about-playing-safely/. – Último acesso Set.2016.

370 Um guia para uma fruição, por parte dos menores, menos arriscada do jogo, poderá ser encontrado, por exemplo, em: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/pokemon-go-parents-guide/ . – Último acesso Set.2016.

371 *Vide* Considerando (38): «*As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças.*».

372 *Vide,* ainda, Considerando (58), parte final: «(…) *Uma vez que as crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente.*».

373 *Vide* Considerando (65): «*Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento.(...) Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto*.».

crianças[374], dos riscos, regras, garantias e direitos associados ao tratamento dos seus dados. Pela nossa parte, notamos que a responsabilidade pela correcta educação de uma criança estará dispersa por diversos actores, dos quais, salientaremos a família, a sociedade, o Estado. É uma responsabilidade de múltiplos actores. À qual todos concorrem.

Por fim, resta saber se, com a entrada em vigor do RGPD, tais acções se realizam e, se realizadas, qual será o seu verdadeiro contributo para uma ***salutar cultura de cibereducação***[375], de todos os actores, públicos/privados, singulares/colectivos, que se pretende fomentar e cultivar.

374 Artigo 57.º, n.º1, alínea b), do RGPD.

375 *«Torna-se pois indispensável nesta conjuntura que a Comissão Nacional de Protecção de Dados (CNPD) emita orientações precisas às escolas sobre os limites legais para o tratamento de dados pessoais, na vertente da sua difusão através da Internet, bem como sobre os procedimentos que devem adotar com vista a aumentar a segurança da informação e a minimizar os riscos de utilização abusiva dos dados pessoais.»*.

Particularmente necessária, e exigente, em abono da verdade, destacamos a Deliberação n.º 1495/2016, tomada em 6 de Setembro de 2016, pela CNPD a propósito da ***Disponibilização de dados pessoais de alunos no sítio da Internet dos estabelecimentos de educação e ensino***. Disponível para consulta em: https://www.cnpd.pt/bin/orientacoes/DEL_1495_2016_dados_alunos_Internet.pdf . – Último acesso, Set.2016.

6. O ESTADO DA ARTE E A ARTE DOS ESTADOS

O conceito de *internet* envolve a noção de rede. É através da rede que é possível conectar uma miríade de terminais, computadores – em sentido lato; telemóveis – *idem*; uma parafernália de novos dispositivos – da *internet das coisas*; que, combinados e à escala global, procedem a uma infindável transferência de dados entre todos. Um dilúvio informacional. Se o meio cresce diariamente em complexidade, não é menos verdade que a nossa dependência regista um acréscimo proporcional a esse crescimento. Aliás, acompanhamos Catarina SARMENTO E CASTRO[376], por exemplo, na consagração do direito à internet, ou de acesso à internet, como um direito fundamental. Este cumpre um desígnio de liberdade ou garantia, precisamente, por permitir que a pessoa exerça, muitos dos seus direitos cívicos de forma em tudo semelhante no mundo virtual[377]. Assim, por exemplo, o voto electrónico; assim a entrega da declaração de rendimentos no portal das finanças; assim muitas das demais ligações que a pessoa estabelece com uma administração pública do estado cada vez mais digital e em rede. Saliente-se, a propósito, a importância da jurisprudência constitucional alemã, expressa pelo *direito fundamental à integridade e confidencialidade dos sistemas de tecnologia da informação,* com a qual se pretende(u) evitar a consumação de um *disruptivo chilling effect* que por receio, obstasse a que a pessoa pudesse aderir à sociedade em rede e da informação[378].

Fruto de uma transformação da sociedade e de uma evolução tecnológica aceleradas, em toda a sua complexidade e dinamismo *à distância de um clique*[379], a sociedade global em

376 Assim, por exemplo, Catarina SARMENTO E CASTRO: «*O Direito à Internet é um direito fundamental instrumental, traduzido num direito de acesso à Internet, que potencia e amplia o exercício de outros direitos e liberdades, incluindo direitos fundamentais, constitucionalmente reconhecidos, como a liberdade de expressão e de comunicação, o direito à informação administrativa, ou o direito de participação democrática*.». Castro, Catarina Sarmento. (2016) Cyberlaw by CIJIC. Disponível em: http://www.cijic.org/wp-content/uploads/2016/06/DIREITO----INTERNET_Catarina-Sarmento-e-Castro.pdf . – Último acesso Set.2016.

377 *Vide* a propósito, a consagração do direito de acesso como um direito humano, em: UNITED NATIONS HUMAN RIGHTS COUNCIL (UNHRC). *THE PROMOTION, PROTECTION AND ENJOYMENT OF HUMAN RIGHTS ON THE INTERNET*. (2016) 32ND SESSION, 30 DE JUNHO. http://www.ohchr.org/EN/Pages/Home.aspx . -último acesso Set.2016.

378 Assim Sousa Pinheiro, *op.cit.*, Pág. 832. *«Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme», com o qual o Tribunal, ao o considerar um direito autónomo, distinguindo-o da informationelle Selbstbestimmung,* procurou promover *a confiança dos utilizadores através da dimensão objectiva que comete aos Estados a tarefa de garantirem a "confidencialidade" e a "integridade" dos sistemas.»*

379 E, assim, DEMCHAK , «*anywhere in the world with unfettered internet access is able to attack in milliseconds due to the global, open, and easy nature of the world's now huge telecommunications systems.(...) capable of starting cascading failures rampaging through large parts of critical national infrastructures at the scale, proximity, and precision of their choosing. They have today the patience,*

rede[380], da comunicação e do conhecimento, releva quer as suas características constantes e crescentes de dependência humana, quer novas modalidades e formas de comissão em ambiente de confronto constante entre a pessoa e a tecnologia. De facto, considerações temáticas à parte, focando-nos no essencial, não poderíamos, por exemplo, em sede de "arte dos estados", não relevar algumas das críticas que STALLMAN[381], por exemplo, elenca quando confessa que a pessoa é usada pela empresa Facebook, e não o seu contrário. "*A arte dos estados*": mesmo que a pessoa, por vezes, *sinta* que domina esta relação, apenas releva para a própria empresa. Com efeito, fruto, inclusive, dos *disclaimers de privacidade que o Facebook outorga,* desde rastreio da pegada digital para efeitos de publicidade dirigida; à migração inadvertida da lista de contactos do Whatsapp; a reconhecimento automatizado facial por via dos *tags* nas fotos; ao *profilling* dos seus clientes; …, de tudo um pouco a empresa vai conseguindo fazer, segmentando a pessoa (cliente, como a ele se refere) em múltiplos "*objectos informacionais*" com os quais vai perseguindo vários modelos de negócio, agigantando ainda mais toda a sua disruptiva capacidade económica.

Extenuante em muitos considerandos, a *internet,* e todas as formas espectaculares que esta nos proporciona de comunicação, tem, de forma disruptiva, alterado a condição social humana. Se, noutros tempos – imemoriais para *millenials*, por exemplo - preza(va)mos uma cultura de maior discrição e privacidade, actualmente, compelidos pela facilidade do «*palco*», alteramos este paradigma de recato, quase por completo. Procuramos, de forma incessante – naquela natural insatisfação humana – e instantânea, prolongar os nossos quinze minutos de fama. A cultura dos *likes* (e *dislikes*) a isso nos compele. As redes sociais mudaram-nos[382]. Julgamos que ORWELL terá sido ultrapassado, precisamente,

---

resources, and convenient access to exploit our cognitive, technological, and institutional disconnects from across the world's immense mass of cyber connections" – DEMCHAK, Chris, «*Conflicting Policy Presumptions about Cybersecurity Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies»,* disponível em: https://www.ciaonet.org/catalog/31656 – Último acesso em Set.2016.

380 Por exemplo, CASTELLS cunhou-a como "Sociedade em rede": «*Una sociedad red es aquella cuya estructura social está compuesta de redes activadas por tecnologías de la comunicación y la información basadas en la microelectrónica (...) La sociedad red es pues una sociedad global. Ello no significa, sin embargo, que las personas de todo el mundo participen en las redes.De hecho, por ahora, la mayoría no lo hace. Pero todo el mundo se ve afectado por los procesos que tienen lugar en las redes globales de esta estructura social»* - CASTELLS, Manuel (2009), *Comunicación Y Poder.*, Traducción María Hernández. Madrid: Alianza Editorial, pp. 50-51.

381 Consideramos impressivas algumas das anotações propugnadas por Richard Stallman, em *Reasons not to use Facebook.* Disponível em: https://stallman.org/facebook.html . - último acesso Out.2016.

382«(…) *the significance of social network sites in the lives of users (...).Collectively, they show how networked practices mirror, support, and alter known everyday practices, especially with respect to how people present (and hide) aspects of themselves and connect with others. The fact that participation on*

por esta vontade humana – *reprimida* - de exibicionismo e *voyeurismo*. Se a realidade ficcional *orwelliana, distópica*[383], de *Oceania*, pressupõe uma forma de controlo social contínuo, manipulativo e hetero-imposto; hoje em dia, o Estado vê esse desígnio muito mais facilitado[384]. Parte de uma condição auto-imposta, pois que o cidadão – virtualizando todas as suas experiências – não consegue desligar-se da rede; e o palco – *qual Ágora de modernidade* – além de aditivo e viciante, vai-se metamorfoseando e absorvendo-nos à margem de qualquer *recato* pessoal. Talvez por desconhecimento das respectivas implicações; talvez sobrelevados pela emoção; certo é que, se por um lado nos prestamos a dizer tudo, a toda a hora, sem qualquer tipo de controlo racional (por exemplo, daquela auto-censura ou *chilling effect* a que nos prestamos quando estamos na presença física de uma outra pessoa), esperando apenas o *consolo* de um *like* ou *dislike*; por outro lado, absorvemos, diariamente, os efeitos extrapolados dos *feed* noticiosos alimentados instantaneamente por *inteligências artificiais* por nós desenhadas e construídas. *Edílico*. Note-se ainda a *gestão da rede*, aprumada nos confins do ciberespaço pelo *divino algoritmo*[385] que tem *autoritariamente* ensombrado[386] –

---

social network sites leaves online traces offers unprecedented opportunities…». Social Networking Sites (Definition): Boyd, Danah M And Elison, Nicole B.. *Journal Of Computer-Mediated Communication*, Volume 13, Issue 1. p. .224.

383 Será assim tão díspar da realidade? Veja-se, por exemplo, BRIN, David, *Transparent Society - Who Watches The Watchers?*.Disponível em: http://www.davidbrin.com/transparentsociety.html . – Ultimo acesso Out.2016.

384 Mais ainda, quando até o simples falar ao telefone está pressuposto numa gravação automática da conversa. Por exemplo, *AT&T Is Spying on Americans for Profit, New Documents Reveal*, disponível em: http://www.thedailybeast.com/articles/2016/10/25/at-t-is-spying-on-americans-for-profit.html. – Último acesso Out.2016.

« (...) Hemisphere isn't a "partnership" but rather a product AT&T developed, marketed, and sold at a cost of millions of dollars per year to taxpayers. No warrant is required to make use of the company's massive trove of data, according to AT&T documents, only a promise from law enforcement to not disclose Hemisphere if an investigation using it becomes public. » .

385 Veja-se, por exemplo, SUNSTEIN, Cass, *Meet the Machines That Know What's Funny*, disponível em: http://www.bloombergquint.com/view/2016/10/04/meet-the-machines-that-know-what-s-funny . – Último acesso Out.2016.

«(...)Researchers led by Mike Yeomans of Harvard University have found that an automated recommender system -- essentially an algorithm based on a lot of data -- does a lot better than human beings (strangers, friends, family or spouses) at guessing what any individual person will find funny. (The team includes two economists, a behavioral scientist and a computer scientist.) Their paper has massive implications for other domains, including medicine, investment choices, regulation, welfare policy, and even the criminal justice system. ».

386 Veja-se, ainda, Pepe ESCOBAR em *A silenciosa ditadura do algoritmo*, disponível em: http://www.cartacapital.com.br/blogs/outras-palavras/a-silenciosa-ditadura-do-algoritmo. – Último acesso Out.2016.

« (...)A maioria dos norte-americanos – para não falar da maioria dos 1,7 bilhão de usuários do Facebook espalhados pelo mundo – ignora que o Facebook canaliza o feed de notícias. As pessoas de fato acreditam que o sistema compartilha instantaneamente, com sua comunidade de amigos, qualquer coisa que é postada. O que nos traz, mais uma vez, à questão chave no front das notícias. Ao ajustar seus algoritmos para modelar as notícias que as pessoas veem, o Facebook tem agora tudo o que é necessário para jogar com todo o sistema político. Como observa O'Neil, "Facebook, Google, Apple, Microsoft, Amazon têm

seguramente pela inculcada cristalização desse mito de que a *internet* nunca esquecerá – a concretização, no virtual, de características tão humanas como esquecer, ser deixado em paz, o arrependimento, perdoar, seguir em frente. Um conjunto significativo de características, tão nossas, tão humanas, que compõem as realidades fácticas mundanas, quotidianas, da vida em sociedade. Mesmo assim, estas têm apresentado resistências diversas[387] à sua concretização na rede, no virtual. O confronto destas realidades, entre outras, tem-nos transportado para uma fronteira de *zombies digitais*[388]. Vemos tudo *online*[389], replicamos tudo, e em tudo acreditamos[390]. De pessoa a um mero autómato, responsivo e *irracional*. E assim, ao de leve, estas *divindades algorítmicas* têm-nos empurrado para um tempo de modernidade do *pós-verdade*.

---

todos uma vasta quantidade de informação sobre grande parte da humanidade – e os meios para nos dirigir para onde queiram".».

387 Veja-se, por exemplo, *Judge decides we don't have any right to privacy,* disponível em: https://nakedsecurity.sophos.com/2016/07/01/judge-decides-we-dont-have-any-right-to-privacy/. – Último acesso Out.2016.

«(...) If you connect your computer to the Internet, like billions of people, then you can't expect any privacy.(...) A federal judge for the Eastern District of Virginia has ruled that the user of any computer connected to the Internet should not have an expectation of privacy because computer security is ineffectual at stopping hackers.».

388 Veja-se, por exemplo: *Facebook has repeatedly trended fake news since firing its human editors*, disponível em: https://www.washingtonpost.com/news/the-intersect/wp/2016/10/12/facebook-has-repeatedly-trended-fake-news-since-firing-its-human-editors/ . – Ultimo acesso Out.2016.

« (...) Facebook trended a news release from the "Association of American Physicians and Surgeons" — a discredited libertarian medical organization — as well as a tabloid story claiming that the Sept. 11 attacks were a "controlled demolition." But if users thought the outrage about Facebook's 9/11 truthering would prompt some reform in Trending, they were mistaken: Less than a week later, Facebook boosted a story about the Buffalo Bills from the well-established satirical site SportsPickle."I'd like to say I expect more from Facebook in advocating truth and informing the citizenry," (...) ».

389 Com os "*perigos*" daí decorrentes. Veja-se, por exemplo: *Angela Merkel: internet search engines are 'distorting perception'*. Disponível em: https://www.theguardian.com/world/2016/oct/27/angela-merkel-internet-search-engines-are-distorting-our-perception. – Último acesso Out.2016.

« (...) The German chancellor said internet users had a right to know how and on what basis the information they received via search engines was channelled to them. Speaking to a media conference in Munich, Merkel said: "I'm of the opinion that algorithms must be made more transparent, so that one can inform oneself as an interested citizen about questions like 'what influences my behaviour on the internet and that of others?'. "Algorithms, when they are not transparent, can lead to a distortion of our perception, they can shrink our expanse of information."».

390 Veja-se, por exemplo, *How technology disrupted the truth,* disponível em: *https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth.* – Último acesso Out.2016.

«(...) "A distinguished Oxford contemporary claims Cameron once took part in an outrageous initiation ceremony at a Piers Gaveston event, involving a dead pig,"(...) "We couldn't get to the bottom of that source's allegations,"(...)"So we merely reported the account that the source gave us ... We don't say whether we believe it to be true."(...) "It's up to other people to decide whether they give it any credibility or not,"(...) It seemed that journalists were no longer required to believe their own stories to be true, nor, apparently, did they need to provide evidence. Instead it was up to the reader – who does not even know the identity of the source – to make up their own mind. But based on what? Gut instinct, intuition, mood?». O efeito bola de neve nas redes sociais foi imediato. A sentença popular, *idem.* A *internet* nunca esquecerá? Perante uma infundada e lacónica suspeita, no fim de contas, existe forma de reparar o descrédito que tal constituiu para a pessoa *David Cameron*?

Relevando, ainda, a nossa própria natureza humana, propensa ao erro, como se não bastasse algum *comportamento imprudente online*[391], as organizações (em todas as suas múltiplas acepções) passaram a olhar para os nossos *vestígios digitais*[392] como *pepitas de ouro*[393]. E por entre estas múltiplas investidas na *caça-ao-ouro*, com efeito, se por um lado do prisma, o Estado acaba por ver a sua, inerente, tarefa securitária[394] e de controlo[395] mais facilitada, conjugando quer propostas legislativas *arrojadas*[396], quer o varrimento

391 Veja-se, por exemplo, *Kim Kardashian foi imprudente na Internet. E nós também somos?*, disponível em: https://www.publico.pt/culturaipsilon/noticia/kim-kardashian-foi-imprudente-na-internet-e-nos-tambem-somos-1746547. – Último acesso Out.2016.
« (...)A partilha de fotos de jóias nas redes sociais, com a localização, foi uma imprudência da celebridade americana Kim Kardashian, contribuindo para que fosse um alvo fácil e apetecível para os homens armados que a amarraram e assaltaram, na segunda-feira, num hotel de Paris.(É a polícia francesa quem o diz.)».

392 E, ainda, *Eres un dato y las empresas te quieren*, disponível em: http://economia.elpais.com/economia/2016/10/07/actualidad/1475854855_806318.html . – Último acesso Out.2016.: *« (...)Nos guste o no, a cada paso que damos dejamos huella en forma de datos. Cuando hacemos deporte con nuestra aplicación cuentakilómetros, cuando usamos una tarjeta, cuando navegamos por Internet, cuando hacemos una llamada o, simplemente, cuando nos movemos con nuestro móvil en el bolsillo. Por no mencionar los que facilitamos voluntariamente al darnos de alta en una red social o al descargar una aplicación. Vivimos en la era del dato y, salvo que hagamos la vida del eremita, liberados de todo dispositivo electrónico, el chorro de información que vamos dejando a nuestro paso no hará sino ganar caudal. Y con el internet de las cosas, el flujo irá a más.».*

393 «*The fact that we can discover new knowledge in existing data by using data mining techniques goes a long way in explaining why big data is a phenomenon that attracts so much attention.(...) Entrepreneurs who work with big data hope that they will be the first to awaken the dormant value that lies hidden in big data datasets. The often used metaphors of data as the new oil and of datasets as goldmines with nuggets of gold hidden inside those datasets.* » - SAX, Marijn. "*Big Data: Finders Keepers, Losers Weepers?*" *in Ethics and Information Technology*, Volume 18, Issue 1, March 2016, p. 27.

394 Por exemplo, *Predicting Terrorism From Big Data Challenges U.S. Intelligence*, disponível em: https://www.bloomberg.com/news/articles/2016-10-13/predicting-terrorism-from-big-data-challenges-u-s-intelligence. – Último acesso Out.2016.
« (…) *mining billions of bits of information and crunching the data to find crucial clues -- is behind a push by U.S. intelligence and law enforcement agencies to harness "big data" to predict crimes, terrorist acts and social upheaval before they happen.(...) "Data is going to be the fundamental fuel for national security in this century,"William Roper, director of the Defense Department's strategic capabilities office, said at a conference in Washington last month.*»

395 Por exemplo, *China wants to give all of its citizens a score*, disponível em: http://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html . – Último acesso Out.2016.
A transparência exigida aos cidadãos e às suas empresas em: «*(...)China's ambitious plans to develop a far-reaching social credit system, a plan that the Communist Party hopes will build a culture of "sincerity" and a "harmonious socialist society" where "keeping trust is glorious."(...) The ambition is to collect every scrap of information available online about China's companies and citizens in a single place – and then assign each of them a score based on their political, commercial, social and legal "credit."».*

396 A exigência estatal de *vitracidade* dos seus cidadãos replica-se sob variadas formas. Como já demos conta, previamente, por exemplo, a propósito da proposta de acesso incondicional às contas bancárias de residentes no território nacional por parte da AT e do Parecer da CNPD respectivo, *supra* em 4.4..

da rede[397] com todo aquele dilúvio informacional que por lá circula[398], por outro lado, as grandes empresas tecnológicas[399], não perdem as oportunidades de negócio que se *abram*[400]. Como se muito disto não bastasse, também, na rede qualquer vestígio, tratado, mapeado e consolidado, passa a valer como *intelligence*[401] ao serviço e à disposição de qualquer um. Um círculo pernicioso de uso e abuso sobre os dados pessoais[402], mais ainda

397 Caso para (re)perguntar até que ponto o eficientismo estadual deverá prevalecer sobre a pessoa. Lembra-nos VOGEL e *«(...)«It is not only the posture of our statue that is designed to overcome corporeality, with its association of uncleanliness; it is, above all, the vitreous figure, the transparency.* ***The individual characteristics of an individual's appearance - skin and hair, muscle and fat - are all missing in the Transparent Man. He is transparent right through; nothing remains hidden.*** *The figure firstly symbolises, in utmost clarity,* ***the claims of an unchallenged natural science that believes itself bound less and less by any secrets****, (...) ».* – VOGEL, Klaus, *"The Transparent Man- Some Comments On The History Of A Symbol"*, Robert Bud, Bernard Finn And Helmuth Trischler (Amsterdam, Harwood Academic Publishers), pp. 45-46.

398 Atente-se, por exemplo, na quantidade de informação de cariz secreto, entretanto, tornada pública, após o "escândalo" envolvendo *Edward Snowden.*

399 Por exemplo*: Facebook, Amazon, Google, IBM and Microsoft come together to create the Partnership on AI,* disponível em: https://techcrunch.com/2016/09/28/facebook-amazon-google-ibm-and-microsoft-come-together-to-create-historic-partnership-on-ai/ . – Ultimo acesso Out.2016.

« (…) ***The world's largest technology companies hold the keys to some of the largest databases on our planet.*** *Much like goods and coins before it, data is becoming an important currency for the modern world.* ***The data's value is rooted in its applications to artificial intelligence. Whichever company owns the data, effectively owns AI. Right now that means companies like Facebook, Amazon, Alphabet, IBM and Microsoft have a ton of power****.(...)*»

400 Por exemplo, *Tech titans are busy privatising our data*, disponível em: https://www.theguardian.com/commentisfree/2016/apr/24/the-new-feudalism-silicon-valley-overlords-advertising-necessary-evil. – Último acesso Out.2016.

«(...) Since data – the fuel of advertising markets – is the source of their profits, ***tech firms are happy to offer, at highly subsidised rates, services and goods that yield even more data.*** *Ultimately there is no limit as to what kind of goods and services those could be: they might have started with browsing and social networking, but they are as happy to track us exercise, eat, drive or even make love: for them, it's all just data – and data means cash. All these subsidies, though, make it hard to understand what the underlying goods and services cost. And as these firms transcend our browsers and smartphones and enter into our homes and cars and bodies, we should expect even more distortion of price signals*.»

401 Por exemplo, *Antigos espiões criam empresa para vender informações a políticos e empresários*, disponível em: http://observador.pt/2016/09/01/antigos-espioes-criam-empresa-para-vender-informacoes-a-politicos-e-empresarios/. – Último acesso Out.2016.

« (…) *A empresa até dá exemplos: "temos um determinado indivíduo, que embora bem-sucedido no seu trabalho ambiciona ir mais além"(...)."Neste caso ter à sua disposição um serviço de Intelligence significa ter do seu lado uma empresa que é capaz de responder com clareza, por exemplo, quem é quem dentro dos ambientes com quem este indivíduo se cruza no seu dia-a-dia. É a possibilidade também de abrir canais, com contactos estratégicos na política ou até na cúpula da empresa para que trabalha para que o seu caminho seja mais fácil".*»

Para os mais curiosos, fica o registo do endereço url onde poderão encontrar estas *secretas privadas* lusitanas: http://www.intellcorp.com/ . – Último acesso Out.2016.

402 O mapeamento e definição de perfil, por parte de *secretas privadas*, com base nos nossos dados pessoais não é, de todo, realidade casuística lusitana. Pior ainda quando comprometida por *valores* justicialistas privados. Veja-se por exemplo: *«(...)VOCÊ que sempre teve a vontade e o desejo de ser um DETETIVE PARTICULAR, e, nunca vislumbrou um meio idôneo de satisfazer o seu desejo, agora VOCÊ tem uma oportunidade única(...)VOCÊ terá, com absoluta certeza, em um diminuto período de tempo, um retorno financeiro consistente e efetivo, além de ter a satisfação de trabalhar num ramo onde a dificuldade de se dirimir as dúvidas, angústias e preocupações dos clientes, se compensa com o prazer da produção das provas respectivas, as quais proporcionam a otimização da VERDADEIRA JUSTIÇA num ESTADO DEMOCRÁTICO DE DIREITO.*». Informação disponível em: Argus Investigação Privada, em http://www.agenciaargus.com/ . – Último acesso Out.2016.

de uso e abuso sobre as próprias pessoas. Sim, porquanto no meio disto tudo estão as pessoas, caminhando virtualmente apáticas (*walking virtually dead*), inabilitadas no exercício efectivo dos seus direitos fundamentais. Caberá «*onde*» o exercício, constitucional, dos nossos direitos e liberdades e garantias fundamentais por esse mundo *online*?

De facto, em abono da verdade, não exortamos a que a Constituição adopte posturas tecnologicamente irrazoáveis. Pelo contrário. O leque de direitos e liberdades e garantias fundamentais parece-nos *suficiente* para salvaguardar o seu exercício por parte das pessoas. Uma interpretação constitucional tecnologicamente neutra, acompanhando Raquel A. BRÍZIDA CASTRO[403] no sentido de que «(…)*o desiderato particular de uma interpretação constitucional tecnologicamente neutra é, precisamente, o de* ***salvar a identidade constitucional, perante as mudanças tecnológicas****, garantindo que o limite interpretativo seja, efetivamente, o texto constitucional. (...)* ***os princípios constitucionais mantêm-se, apesar das novas tecnologias, deslegitimando qualquer tentativa de mutação informal da Constituição****, gerada pelo medo ou mera conveniência da indefinição, encorajadora de interpretações arrojadas ou, simetricamente, demasiado contidas.* ***Os Princípios fundamentais estruturantes de um Estado de Direito Democrático não podem ser desprezados na voragem de uma qualquer pretensão regulatória*** *ou de reparação judicial.*». Perante tal azáfama na rede, teremos forma de (re)ganhar alguma posição de controlo da nossa intrínseca dignidade humana *online*?

A este propósito, atentemos, em particular, no exemplo, do direito a ser esquecido (*Right to Be Forgotten* - RTBF). Este, aparentemente, e a sua execução, suscitam, desde logo, questões técnicas de difícil conciliação. Não impossíveis, mas de difícil execução. Destacaríamos, desde logo, a praticabilidade – ou não – do argumento elencado pela *Google*: como responder tecnicamente de forma satisfatória a cerca de um (1) milhão de pedidos para desindexar cerca de 1.6 milhões de *URLs*? Principalmente, quando os

403 disponível em: CASTRO, Raquel A. Brizida (2016) "*Constituição E Ciberespaço: Argumentos Para Um "Direito Constitucional Do Inimigo"?" in Cyberlaw By Cijic*. Disponível Em: http://www.cijic.org/wp-content/uploads/2016/01/constitui----o-e-ciberespa--o_argumentos-para-um----direito-constitucional-do-inimigo---.pdf.

pedidos, grosso modo, cerca de 96%[404], incidem sobre informação pessoal contida em *social media or profiling sites*?

De facto, conciliar pedidos de desindexação, pressupostos numa virtude – *ímpar* – humana de tudo partilhar com o seu semelhante, naquele paradoxo de privacidade de "*partilho tudo na rede, mas reclamo privacidade*", assume-se como uma variável *sufocante*. Por um lado, o *input* inicial parte da própria pessoa: esta publica; arrependida, solicita a sua desindexação. A análise e posterior desindexação parte, após uma interpelação (outro *input*) do visado, da interpretação que um dado gigante tecnológico faça sobre aquele caso em particular[405]. Estranho? Talvez não. O *código* assim o prescreve. Depois, e ainda, consideremos a singularidade do *Streisand effect*[406]. *I.e.*, aquele fenómeno que consiste numa maior dispersão da "*informação*" cujo único intuito inicial passaria por "*esconder*" e não divulgá-la. Ou seja, num dado momento, uma pessoa (ou organização), procura *esconder, remover ou apagar* uma dada informação, a qual, pela publicidade que lhe é entretanto "*conferida*", produz o resultado final precisamente contrário (um pouco como o que *Mário Costeja* acabaria por experienciar, após ter prosseguido com o seu caso em Tribunal e nas instâncias judiciais europeias; assim, ainda, por exemplo o caso de Olivier G. que trataremos de seguida; entre muitos outros casos). Má *publicidade*, boa *publicidade*, no presente, a facilidade de dispersão de um facto, verdadeiro ou falso, condiciona o exercício de um desenvolvimento da personalidade em liberdade, bem como, acomete uma ingerência desmesurada na esfera da reserva da intimidade da vida privada e familiar.

Nem tudo, obviamente e em abono da verdade, se nos revela assim tão *distópico*. Com efeito, importa considerar algumas notas significativas para que *o direito a ser esquecido não passe no esquecimento*, depois de todo o palco que o TJUE lhe conferiu em 2014, e da sua expressa jurídico-positivação presente, no RGPD. Vamos por partes.

404 Por exemplo, *Google's Data On the the Right to be Forgotten* em: http://sytpp.github.io/rtbf/index.html . - Ultimo acesso Out.2016.

405 Veja-se, por exemplo: *Facebook to consider public interest before removal of posts violating guidelines*, disponível em: https://www.theguardian.com/technology/2016/oct/24/facebook-public-interest-removal-posts-violating-guidelines . – Útimo acesso Out.2016.

406 Assim, MINHUI XUE et al., em *The Right To Be Forgotten In The Media: A Data-Driven Study.* Disponível em: http://engineering.nyu.edu/files/RTBF_Data_Study.pdf. – Último acesso Out.2016.

A) Por um lado, consideramos a decisão tomada pelo *Court of Cassation* belga, a propósito do caso *Olivier G v Le Soir*[407]. O caso, em traços genéricos, envolvia a pessoa *Olivier. G* e o jornal *Le Soir*. Na versão *online* do jornal, no arquivo digital, continuava a constar uma notícia de 1994, dando conta de um acidente fatal, onde a pessoa *Olivier G.,* alcoolizado, teria morto uma outra pessoa num acidente de viação. *Olivier,* tendo já cumprido a sua pena por este facto na vida real, continuava a carregar a cruz desse trágico acidente, no mundo *online*. Solicitou, por tal, que o jornal *Le Soir* o anonimizasse desse registo em arquivo. Perante a recusa do jornal, recorreu para as instâncias judiciais. É precisamente aqui que esta decisão do tribunal superior belga releva.

Dando acolhimento aos argumentos de *Olivier,* a *Court of Cassation* ordenou a anonimização deste do arquivo do jornal. Sustentou tal posição em cinco (5) conclusões:

(i) A divulgação dos factos do acidente ocorrido em 1994 não tinham no presente interesse noticioso;

(ii) *Olivier* não exercia nenhum cargo público;

(iii) Remover o nome de *Olivier* dessa notícia não tinha qualquer impacto quanto à essência dessa notícia;

(iv) Por conseguinte, os argumentos baseados na preservação do arquivo *online,* com todos os elementos da notícia, não faziam sentido, uma vez que o arquivo físico não seria objecto desta anonimização;

(v) Não havia interesse do público em conhecer a identidade da pessoa responsável por um trágico acidente de viação que havia ocorrido há mais de 20 anos.

Lapidar na argumentação, o Tribunal belga, não escamoteando a verdade dos acontecimentos, procedeu à reparação dos danos reputacionais quanto à pessoa *Olivier G.,* que ainda persistiam no tempo, fruto da arquitectura *online*. Mesmo considerando o *Streisand effect*, a condição de pessoa prevaleceu sobre a de "*objecto de informações*", fazendo-se justiça quanto a "parte" do seu "*arquivo e pegada digital*".

407 Processo n° C.15.0052.F, Acórdão de 29 April 2016 - Acórdão disponível, em francês, em: https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf . – acedido em Out.2016.

Naturalmente, esta decisão suscitou logo a crítica *eficaz* de "*censura à liberdade de expressão e de informação*" [408]. Mas, como afirma Norberto ANDRADE[409], no confronto entre o direito a ser esquecido e a liberdade de expressão e informação, por regra, tais objecções representam apenas o paradigma clássico revivalista do conflito da doutrina americana. Relevam as pessoas. Não os factos. Mesmo que isto seja difícil de querer compreender. Mais, quer no *caso Costeja,* quer neste *caso Olivier*, o que realmente está em causa é a possibilidade de cada uma destas pessoas poder ser diferente daquilo que foi no seu passado. É um "*direito a renascer*". E este "renascer", é um instrumento de correcção e de reprojecção individual que cada pessoa deve poder exercer, mesmo no contexto *online*[410].

B) Em segundo lugar, e complementarmente, atento, em particular, o novo quadro regulatório instituído pelo RGPD, consideramos fundamental a protecção da pessoa no contexto *online* irradiada pelo direito à identidade informacional ("*um direito guarda-chuva*") e positivamente alavancado no leque de direitos que o Regulamento considera, os quais já fomos dando conta supra. Independentemente da perspectiva com que se encare a enumeração (exemplificativa) destes direitos, a portabilidade, a informação e o acesso, a rectificação, a limitação, o apagamento, o direito a ser esquecido, todos eles

---

408 Aqui, com ênfase, a propósito da Liberdade de expressão, numa outra perspectiva de protecção constitucional de um *direito a mentir* nas discussões doutrinárias americanas, Garrett EPPS: «*The idea that lies are part of "freedom of speech" or "of the press" seems wrong. Lies—even lazy falsehoods—make finding the truth harder, erode mutual trust, and harm individuals and groups. Some can even lead to private violence or public disorder. Why would free speech protect them? Under U.S. law, many falsehoods—even some deliberate lies—receive the full protection of the First Amendment. That is true even though "there is no constitutional value in false statements of fact," as Justice Lewis Powell Jr. wrote for the Supreme Court in 1974. Nonetheless, the Court has often refused to allow government to penalize speakers for mistakes, sloppy falsehoods, and lies. Political lies are strongly protected; but even private lies sometimes are as well.(...) That's not because there's any "constitutional value" in false statements of fact but because the cure—government control of what can be said in politics—is far worse than the disease. To enforce this law, the tribunal would summon the speaker and demand proof that the false statement was not a deliberate lie. That process will inevitably suppress some true statements along with the false and frighten some meritorious speakers into silence; those suppressions are, over time, likely to be skewed toward speech that criticizes government*.»
Disponível em: http://www.theatlantic.com/politics/archive/2016/08/does-the-first-amendment-protect-deliberate-lies/496004/ . – último acesso Set.2016.

409 ANDRADE, Norberto Nuno Gomes de (2012) *Oblivion: The Right To Be Different ... From Oneself. Reproposing The Right To Be Forgotten*, p. . 130.

410 *Idem. Op.cit*. - «*The right to be forgotten as an attempt to manipulate some kind of Internet objectivity or collective society memory is a somewhat unconvincing argument, if not unfounded. First, the notion of objectivity is rather controversial coming from a search engine that organizes its search listings through enigmatic and non-transparent algorithms. Second, it seems unbalanced to deny the individual the right to erase personal information that is, among other criteria discussed below, not newsworthy or of historical relevance, only for the sake of sustaining a supposedly collective memory. In view of this, I believe there is an overstretched emphasis on an unsounded collective interest to the detriment of a needed individual interest, such as the right to be different from who one was before.», Ibidem,* p. . 131.

constituem *ferramentas* de controlo dos dados pessoais à disposição da pessoa titular desses dados.

É por isso que deveremos encarar o "*direito ao esquecimento*" como um instrumento do direito a uma identidade informacional (*online*), suficientemente capaz de nos permitir a construção da pessoa que queremos seguir, na nossa essência, diferente dos outros semelhantes, com a possibilidade de nos reconstruirmos, tantas vezes quanto as necessárias, sempre que o projecto que estejamos a seguir, apresente *falhas*. Desde logo, para o próprio. Mesmo no contexto *online*, cada vez mais presente na nossa vida. Estas "*falhas*", comprimidas em "identidades passadas", devem poder ser afastadas e substituídas pelas "novas identidades" que decidamos erigir[411]. É pois a possibilidade de exercício deste "*direito a começar de novo*", alavancado na conjugação dos *artigos 35.º e 26.º da CRP, abrangendo as posições jurídicas que se expressam desde a protecção da informação pessoal até ao livre desenvolvimento da personalidade,* que *o "direito à identidade informacional" vingará num universo cibernético povoado de relações pessoais em rede* (SOUSA PINHEIRO, 2015)[412]. Aquilo que Norberto ANDRADE caracterizou como *"a mudança de paradigma da privacidade para a identidade"*[413]. Porque o radical deve estar sempre focado na pessoa, não no "*objecto de informações*" com que o estado da arte o encara, e a arte dos estados por vezes a isso poderá induzir.
É pois sintomático que, no caso português, em sede de futura revisão constitucional, consideremos a necessidade de constitucionalização deste direito, "*guarda-chuva*", à identidade informacional. A sua constitucionalização, permitiria, por um lado, a consciencialização de *controlo* por parte da pessoa, deslocado do foco nos "dados pessoais" e da "protecção dos dados" centrando-se nesta em si mesma considerada, num contexto *online*. Por outro lado, "*as falhas originais*" e interpretações avulsas, tendentes a desconsiderar a efectividade de tutela da pessoa em detrimento da *sedutora* condição de

411 *Idem. Op.cit*. - « ***the right to new beginnings, the right to start over, with a clean slate, and the right to selfdefinition****, preventing the past from excessively conditioning our present and future life. The right to be forgotten can therefore be considered an important legal instrument to both de- and reconstruct one's identity,* ***to provide the opportunity to re-create oneself****, exerting better control over one's identity.*» - *Ibidem*, p. 134
412 SOUSA PINHEIRO, *op.cit,* p. 828.
413 ANDRADE, Norberto, *op.cit*. - *«(...)the right to oblivion, conceptualized and supported by the right to identity, will present a stronger rationale and justification to attain a better, fairer balance with other competing rights and interests.(...) The paradigm shift from privacy to identity also reinforces and widens the applicability of the right to oblivion, encompassing areas and situations that it otherwise could not cover*.» - *Ibidem,* pág. 134.

"*objecto de informações*", seriam afastadas, cumprindo-se o desígnio de positivação do direito à identidade informacional que perscrutamos.

7. CONCLUSÕES

Um dos grandes desafios de modernidade decorrerá da busca do justo equilíbrio entre a *segurança do estado*[414] e a mínima restrição às garantias e liberdades fundamentais dos cidadãos[415]. O objectivo almejado não será fácil de atingir, mais das vezes porque o «*estado tudo quer prever*[416]» sendo que a opção por uma metodologia de intercepção massiva e indiscriminada de telecomunicações, a reboque da invocação do objetivo da segurança nacional ou do *combate ao terrorismo*, assume-se como condição e fundamento bastante[417], assertivo e *tolerado*[418] pela população em geral.

Se, por um lado, o panorama actual concentra esta constatação, não é de todo descurável o facto de, do outro lado da observação, verificarmos que existe uma mecânica intrincada de *adoração* da *algoritmocracia divina,* suportada por uma cada vez mais perspicaz

414 *«An avidity to punish is always dangerous to liberty. It leads men to stretch, to misinterpret, and to misapply even the best of laws. He that would make his own liberty secure must guard even his enemy from oppression; for if he violates this duty he establishes a precedent that will reach to himself».* Thomas Paine, *A Dissertation on the First Principles of Government* (1795). disponível em: https://archive.org/details/dissertationonfi00pain .Pág. 32. – último acesso Out.2016.

415 Assim, FIGUEIREDO DIAS, analisando os problemas de articulação do direito à informação com a protecção da intimidade da vida privada e a sua potenciação na *sociedade do risco e da informação*, nomeadamente no ciberespaço - "Direito à Informação, Proteção da Intimidade e Autoridades Administrativas Independentes*", in Estudos em homenagem ao Prof. Doutor Rogério Soares,* Stvdia Ivridica 61, Ad Honorem-1, Boletim da Faculdade de Direito, Universidade de Coimbra: Coimbra Editora, 2001, pp. 652 e ss.

416 Conforme, aliás, notou Cristina MÁXIMO DOS SANTOS, quando «*" algumas tendências securitárias da actualidade (...) trazem consigo a ideia perversa de que a vigilância permanente tudo resolve porque tudo prevê."*» - "*As novas tecnologias de informação e o sigilo das telecomunicações*", in *RMP*, nº99, pág.99.

417 Pela nossa parte, e à luz da doutrina e Constituição nacional, ter consciência da existência de riscos não poderá significar a concessão de um mandato de poderes ilimitados às instituições políticas e/ou juridicamente constituídas. Até porque a «*cultura do medo*» ajuda a criar a consciência da tolerância de certas intrusões, claramente abusivas por parte do estado. Com propriedade, por exemplo, Benjamim SILVA RODRIGUES nota que « (…) *a eclosão do direito à autodeterminação informacional e comunicacional, traduz-se na faculdade do titular controlar e dispor da sua informação pessoal e de poder comunicar, como quiser (meio técnico), com quem quiser (escolha do interlocutor), quando quiser (tempo), o que quiser (conteúdo), sem que veja cerceado o seu direito no acto comunicacional pela ingerência de um terceiro. O direito fundamental acabado de enunciar encontra a sua expressão no texto constitucional, nos artigos 34.º e 35.º, sob as epígrafes, "Inviolabilidade do domicílio e da correspondência" e "Utilização da informática", respetivamente.*» - SILVA RODRIGUES, Benjamim, "*A Monitorização De Dados Pessoais De Tráfego Nas Comunicações Electrónicas"* (jul./Dez. 2007), *in Raízes Jurídicas Curitiba, v. 3*, n. 2, p. 71.

418 Num mundo hiperconetado e, por conseguinte, em constante perseguição de informação e de notícia, algumas minorias impõem, através das redes sociais, a *ditadura* da sua liberdade de expressão, configurando verdadeiras formas de *bullying* social. Cria-se um ambiente de perigo ou de medo com vista à legitimação de ingerências inadmissíveis nos direitos e liberdades fundamentais da pessoa.

inteligência artificial[419]. A alegada *oposição* entre o *mundo* da tecnologia e o mundo do direito apenas revela esta velocidade temporal assíncrona. Não acompanhando o ritmo temporal da tecnologia, disruptiva, avassaladora, o direito ainda tende a perder-se em querelas e discussões doutrinárias de pormenor, descurando a substancialidade dos seus propósitos: a pessoa humana. Talvez o novo Regulamento Geral de protecção de dados inculque uma realidade diferente. Estamos confiantes. Alargando o escopo de protecção da pessoa, por acréscimo, dos seus dados, e controlando as famintas investidas organizacionais sobre estes, admitimos que a pessoa possa (re)exercer assertiva e conscientemente os seus direitos. No caso português, admitimos, ainda, a constitucionalização do direito à identidade informacional em sede de futura revisão constitucional. Conhecendo as "*regras*", poderemos perspectivar o nosso comportamento futuro em respeito por estas. É um facto, de *la palisse*.

Os desafios postos a ambas as realidades (direito e tecnologia), provocadores da própria essência da natureza humana, insistimos, apenas denotam uma aparente distanciação. Por duas razões basilares: se ambas devem respeito a um determinado código, que enforma toda a abrangência destas realidades, feito pelas pessoas; ao mesmo tempo, não poderão negligenciar que estão – exclusivamente - ao serviço da pessoa. Com efeito, de forma simplista, diríamos que da mesma forma que um *engenheiro informático* deverá conformar-se a um determinado código na elaboração de um dado programa de *software,* ou no *assemblance* de *hardware e design de software*[420]*,* que ulteriormente será posto ao serviço da pessoa humana; a um *jurisprudente* exige-se esse mesmo nível de conformação a um *código – Ius Cogens* – que é a dignidade humana, pois que a norma que se revelar deverá respeitar toda a essência de dignidade da pessoa humana. Até porque, complementando-se, o seu propósito deverá passar, em exclusivo, pelo auxílio à pessoa na sua constante luta para suprimir as suas naturais imperfeições – o poder ter *o direito a "renascer"*, o poder ter o direito a projectar a sua identidade informacional.

Compatibilizar a dimensão garantística, inerente ao direito à identidade informacional, com a flexibilidade regulatória que as tecnologias reclamam, sob pena de ineficácia,

419 Assim, por exemplo, *The Rise of Conscious Combinatorial Technology*, disponível em: https://medium.com/twenty-one-hundred/the-rise-of-conscious-combinatorial-technology-94b8e9787cb0#.scwel3vmp. – Último acesso Out.2016

420 Desde logo, com a afirmação efectiva do conceito de *privacy by design*, *privacy by default*.

aparenta um *obstáculo* à eficácia tecnológica. Compreendemos. Tal afirmação, porém, a nosso ver, reclama um equilíbrio delicado, justo, entre forças poderosas e em constante movimento. Secularmente, pela força disruptiva das tecnologias e de outros fenómenos, foi preciso travar desequilíbrios. Mas é, precisamente, aqui que reside toda a essência das realidades tecnológica e do direito: na pessoa humana. Assumindo que *a internet nunca esquece*, importa sublinhar, que nunca esqueça que deverá estar sempre ao exclusivo serviço da pessoa. E não o seu contrário. O paradoxo revelado neste mito de que «*a internet nunca esquece*», apresenta-se-nos enviesado. *I.e.*, sendo «esquecer» uma característica tão distintivamente humana; sendo a internet uma ferramenta criada pelo homem; teremos chegado a um tempo em que a ferramenta quer obrigar o seu criador a nunca esquecer; a negar as suas próprias características, inatas? De todo.

É assim, pois, numa simbiose entre a presente aparente dicotomia, que urge sedimentar um direito à identidade informacional (*online*), superando as «*falhas originais*» doutrinárias, balizando a dispersão entusiástica tecnológica e, no fundo, aproximando-o da pessoa humana que lhe confere "*existência*". Porque a pessoa não é um "*mero objecto de informações*", mas um fim de dignidade humana que cumpre sempre salvaguardar.

BIBLIOGRAFIA

II – Doutrina Internacional

ACQUISTI, Alessandro/**GROSS**, RALPH. (2006), "Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook", *in Privacy Enhancing Technologies,* VOLUME 4258 OF THE SERIES LECTURE NOTES IN COMPUTER SCIENCE. SPRINGER BERLIN HEIDELBERG, pp. 36-58;

AMBROSE, Meg Leta

- (2012) "You Are What Google Says You Are. The Right To Be Forgotten and Information Stewardship", in International Review of Information Ethics, Vol. 17, pp. 20-31;
- (2013) "It.s About Time. Privacy, Information Life Cycles and The Right To Be Forgotten", in Stanford Technology Law Review, Vol.16, N.2., pp.369-422;

ANDRADE, Norberto Nuno Gomes de (2012),"*OBLIVION: THE RIGHT TO BE DIFFERENT ... FROM ONESELF REPROPOSING THE RIGHT TO BE FORGOTTEN"* – Monograph - *VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet»*. IDP, Revista De Internet, Derecho Y Politica, pp. 122-137;

ARTHUR, W. Brian (2009), *The Nature Of Technology: What it is and How it Evolves*, NEW YORK: FREE PRESS.

BERNARDO, PAULO, E LINDOSO E LIMA (2015) "*ASPECTOS JURÍDICOS DOS DADOS E PERFIS EM REDES SOCIAIS: A TUTELA CONSUMERISTA, O MARCO CIVIL DA INTERNET E O PROJETO DE LEI 281/2010*", *in RJLB- REVISTA JURÍDICA LUSO BRASILEIRA,* n.º2, disponível online em: http://www.cidp.pt/revistas/rjlb/rjlb-2015-02

BERNERS-LEE, TIM (1989) *INFORMATION MANAGEMENT: A PROPOSAL*;

BORKING, JOHN J (2011) "*WHY ADOPTING PRIVACY ENHANCING TECHNOLOGIES (PETS) TAKES SO MUCH TIME*", *in COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE, SPRINGER*, pp. 309-341;

BOYD, DANAH M AND **ELISON**, NICOLE B. (2008) "*SOCIAL NETWORK SITES_DEFINITION_HISTORY_AND SCHOLARSHIP*", *in JOURNAL OF COMPUTER-MEDIATED COMMUNICATION,* VOLUME 13, ISSUE 1, pp. 210.230;

BRIN, David (1989) *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM ?,* BASIC BOOKS; FIRST TRADE PAPER ED EDITION;

CAMPBELL, Roy; JALAL AL-MUHTADI (2003) "PRASAD NALDURG; GEETANJALI SAMPEMANE; M. DENNIS MICKUNAS. *TOWARDS SECURITY AND PRIVACY FOR PERVASIVE COMPUTING*", *in M. OKADA ET AL., SPRINGER-VERLAG BERLIN HEIDELBERG 2003, pp. 1-15;*

CASTELLS, Manuel (2009) *COMUNICACIÓN Y PODER,* TRADUCCIÓN MARÍA HERNÁNDEZ. MADRID: ALIANZA EDITORIAL;

CAVOUKIAN, Ann

- (2012) *PRIVACY BY DESIGN: FROM RHETORIC TO REALITY* – disponível online em. https://www.ipc.on.ca/wp-content/uploads/Resources/PbDBook-From-Rhetoric-to-Reality.pdf;
- (2012) *PRIVACY BY DESIGN AND USER INTERFACES: EMERGING DESIGN CRITERIA – KEEP IT USER-CENTRIC* - disponível online: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces_Yahoo.pdf;
- *A REGULATOR'S PERSPECTIVE ON PRIVACY BY DESIGN* - disponível online: https://fpf.org/wp-content/uploads/A-Regulators-Perspective-on-Privacy-by-Design.doc;
- *INTERNATIONAL COUNCIL ON GLOBAL PRIVACY AND SECURITY, BY DESIGN (GPS by DESIGN),* disponível em: http://gpsbydesign.org/

CHU, NATASHA. *PROTECTING PRIVACY AFTER DEATH*. (SEPTEMBER 2015) NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY, VOLUME 13, NUMBER 2, PP. 254-276

CHURCH, SCOTT H. (2013) "*DIGITAL GRAVESCAPES: DIGITAL MEMORIALIZING ON FACEBOOK*.", in INFORMATION SOCIETY, N 29, PP. 184–189;

JANEIRO, DOMINGO BELLO (2001) "*LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL DERECHO COMUNITARIO*", in ANUARIO DA FACULTADE DE DEREITO DA UNIVERSIDADE DA CORUÑA, Nº 5, PP. 133-156;

JEWEL, LUCILLE A. (2011) "*YOU'RE DOING IT WRONG: HOW THE ANTI-LAW SCHOOL SCAM BLOGGING MOVEMENT CAN SHAPE THE LEGAL PROFESSION", in MINNESOTA JOURNAL OF LAW, SCIENCE & TECHNOLOGY.* PP. 239-278;

KEEN, ANDREW (2012) *DIGITAL VERTIGO: HOW TODAY'S ONLINE SOCIAL REVOLUTION IS DIVIDING, DIMINISHING, AND DISORIENTING US*;

KIRSCH, MATTHEW S. (2011) "*DO-NOT-TRACK: REVISING THE EU'S DATA PROTECTION FRAMEWORK TO REQUIRE MEANINGFUL CONSENT FOR BEHAVIORAL ADVERTISING*", *in RICHMOND JOURNAL OF LAW & TECHNOLOGY,* VOLUME XVIII, ISSUE 1, disponível em: http://jolt.richmond.edu/v18i1/article2.pdf

KOOPS, BERT-JAAP.

- (2014) "*THE TROUBLE WITH EUROPEAN DATA PROTECTION LAW*", *in International Data Privacy Law.* Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692;
- (2011) "*FORGETTING FOOTPRINTS, SHUNNING SHADOWS. A CRITICAL ANALYSIS OF THE "RIGHT TO BE FORGOTTEN" IN BIG DATA PRACTICE", in Tilburg Law School Legal Studies Research Paper Series* , No. 08/2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719

KOOPS, BERT-JAAP. and **LEENES**, RONALD E.. (2005) *'CODE' AND PRIVACY - OR HOW TECHNOLOGY IS SLOWLY ERODING PRIVACY*", *ESSAYS ON THE NORMATIVE ROLE OF INFORMATION TECHNOLOGY,* T.M.C. ASSER PRESS, THE HAGUE. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=661141

KORENHOF, PAULAN (2013) "*FORGETTING BITS AND PIECES: AN EXPLORATION OF THE 'RIGHT TO BE FORGOTTEN' AS IMPLEMENTATION OF 'FORGETTING' IN ONLINE MEMORY PROCESSES*", *in Tilburg Law School Legal Studies,* Research Paper No. 014/2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326475

KORENHOF, PAULAN and **GORZEMAN,** LUDO (2015) *WHO IS CENSORING WHOM? AN ENQUIRY INTO THE RIGHT TO BE FORGOTTEN AND CENSORSHIP* - Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2685105

LESSIG, LAWRENCE

- (1996) *READING THE CONSTITUTION IN CYBERSPACE* - Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=41681;
- (1999) *CODE AND OTHER LAWS OF CYBERSPACE*, NEW YORK: BASIC BOOKS.

LESSIG, LAWRENCE and **LEMLEY**, MARK A. (2000) *THE END OF END-TO-END: PRESERVING THE ARCHITECTURE OF THE INTERNET IN THE BROADBAND ERA,* U.C. Berkeley Public Law and Legal Theory Research Paper No. 36. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=247737

LUCAS MURILLO DE LA CUEVA, PABLO

- (2008) "*EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA Y LA PROTECCIÓN DE DATOS PERSONALES*", *in AZPILCUETA: CUADERNOS DE DERECHO*, Nº. 20, pp. 43-58;

- (2007) "*PERSPECTIVAS DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA", in IDP REVISTA DE INTERNET*, DERECHO Y POLÍTICA, Nº. 5, pp. 18-32;

- (2003) "*LA CONSTITUCIÓN Y EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA*", *in CUADERNOS DE DERECHO PÚBLICO*, Nº 19-20 (EJEMPLAR DEDICADO A: PROTECCIÓN DE DATOS), pp. 27-44;

- *LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL EN EL HORIZONTE DE 2010*, disponível em: http://dspace.uah.es/dspace/bitstream/handle/10017/6440/proteccion_murillo_afdua_2009.pdf?sequence=1&isallowed=y

LUCENA, CLÁUDIO (2016) *IGORITHM: YOU ARE WHAT YOU BROWSE* - Disponível em: https://prezi.com/t_gbvocr0rgx/igorithm-you-are-what-you-browse/

MAYER-SCHÖNBERGER, VIKTOR (2009) *DELETE THE VIRTUE OF FORGETTING IN THE DIGITAL AGE.*, PRINCETON UNIVERSITY PRESS, PRINCETON AND OXFORD, - blog VMSWEB, disponível em: http://www.vmsweb.net/;

CONNOR, JOHN (2011) "*DIGITAL LIFE AFTER DEATH: THE ISSUE OF PLANNING FOR A PERSON'S DIGITAL ASSETS AFTER DEATH*", *in Texas Tech School of Law Legal Studies* Research Paper No. 2011-02, disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1811044

CRAWFORD, SUSAN (1983) *THE ORIGIN AND DEVELOPMENT OF A CONCEPT: THE INFORMATION SOCIETY*. HTTPS://WWW.NCBI.NLM.NIH.GOV/PMC/ARTICLES/PMC227258/PDF/MLAB00068-0030.PDF

DEMCHAK, CHRIS (2010) *CONFLICTING POLICY PRESUMPTIONS ABOUT CYBER SECURITY: CYBER–PROPHETS, –PRIESTS, –DETECTIVES, AND –DESIGNERS, AND STRATEGIES FOR A CYBERED WORLD* - disponível em: https://www.ciaonet.org/catalog/31656

DONEDA, DANILO (2008) *PRIVACIDADE, VIDA PRIVADA E INTIMIDADE NO ORDENAMENTO JURÍDICO BRASILEIRO. DA EMERGÊNCIA DE UMA REVISÃO CONCEITUAL E DA TUTELA DE DADOS PESSOAIS*, Âmbito Jurídico, Rio Grande,

XI, n. 51. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460 .

GÜRSES, SEDA (2014) *CAN YOU ENGINEER PRIVACY? ON THE POTENTIALS AND CHALLENGES OF APPLYING PRIVACY RESEARCH IN ENGINEERING PRACTICE*, COMMUNICATIONS OF THE ACM, VOLUME 57 ISSUE 8, pp. 20-23;

HAYTHORNTHWAITE, CAROLINE (2005) "*SOCIAL NETWORKS AND INTERNET CONNECTIVITY EFFECTS"*, *in INFORMATION, COMMUNICATION & SOCIETY JOURNAL,* VOL.8, ISSUE 2, pp. 125-147;

IGLEZAKIS, IOANNIS

- *(2014) THE RIGHT TO BE FORGOTTEN IN THE GOOGLE SPAIN CASE (CASE C-131/12): A CLEAR VICTORY FOR DATA PROTECTION OR AN OBSTACLE FOR THE INTERNET?* - Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323;
- *(2014) DIGITAL FORGETTING IN THE AGE OF SOCIAL MEDIA: ESTABLISHING A COMPREHENSIVE RIGHT TO CYBER-OBLIVION*) disponível em: http://www.academia.edu/8408079/Digital_Forgetting_in_the_Age_of_Social_Media_Establishing_a_Comprehensive_Right_to_Cyber-Oblivion

MINHUI XUE, GABRIEL MAGNO, EVANDRO CUNHA, VIRGILIO ALMEIDA, AND KEITH W. ROSS. *THE RIGHT TO BE FORGOTTEN IN THE MEDIA: A DATA-DRIVEN STUDY* (2016). PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES. PP. 389–402 disponível em: http://engineering.nyu.edu/files/RTBF_Data_Study.pdf

NETANEL, NEIL WEINSTOCK. (2000) "*CYBERSPACE 2.0*." *, in TEXAS LAW REVIEW,* VOL. 79. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=252557;

OTEIZA, EDUARDO (1999) «*INFORMACIÓN PRIVADA Y HABEAS DATA*», *in Revista Jurídica de la Universidad de Palermo.* PP-167-181. disponível em:

http://www.palermo.edu/derecho/publicaciones/pdfs/revista_juridica/Especiales_SELA/SELA%201998%20-%20Ed%201999/04SELA98Juridica13.pdf ;

PAINE, THOMAS. (1795) *A DISSERTATION ON THE FIRST PRINCIPLES OF GOVERNMENT*. Versão digitalizada disponível em: https://archive.org/details/dissertationonfi00pain .

PALAZZI, PABLO A. *(2016) "CRITERIOS PARA IMPLEMENTAR EL DERECHO AL OLVIDO EN INTERNET: COMENTARIO A LAS DIRECTRICES DEL GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA UNIÓN EUROPEA***", *in Cyberlaw by CIJIC*. Disponível em: http://www.cijic.org/wp-content/uploads/2016/01/PABLO-A-PALAZZI.pdf ;

POSTMAN, NEIL (1993) *TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY*, (1993) FIRST VINTAGE BOOKS EDITION;

PRENSKY, MARK. *DIGITAL NATIVES, DIGITAL IMMIGRANTES*. (October 2001) On the Horizon (MCB University Press, Vol. 9 No. 5.) disponível em: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf;

PUCCINELLI, ÓSCAR R. (2016) "*LA RESPONSABILIDAD DE LOS PROVEEDORES DE SERVICIOS Y DE LOS USUARIOS DE INTERNET POR PUBLICACIONES OFENSIVAS: UN BREVE MUESTRARIO JURISPRUDENCIAL", in Cyberlaw by CIJIC.* Disponível em: http://www.cijic.org/wp-content/uploads/2016/01/OSCAR-PUCCINELLI.pdf ;

RODRIGUES, BENJAMIM SILVA (2007) *A MONITORIZAÇÃO DE DADOS PESSOAIS DE TRÁFEGO NAS COMUNICAÇÕES ELECTRÓNICAS,* (JUL./DEZ. 2007), in RAÍZES JURÍDICAS. *CURITIBA, V. 3*, N. 2.

ROSEN, JEFFREY **(2012)** *THE RIGHT TO BE FORGOTTEN*, SYMPOSIUM ISSUE, STANFORD LAW REVIEW ONLINE, VOL.64, pp. 88-92;

SALKIN, ALLEN, *WHAT'S IN A NAME? ASK GOOGLE*. (25/Nov.2011). Artigo de opinião no NYTimes, disponível em: http://www.nytimes.com/2011/11/27/fashion/google-searches-help-parents-narrow-down-baby-names.html;

SAX, MARIJN (2016) "*BIG DATA: FINDERS KEEPERS, LOSERS WEEPERS?"* (MARCH 2016), *in ETHICS AND INFORMATION TECHNOLOGY,* VOLUME 18, ISSUE 1, pp. 25-31; disponível em *open access* em: http://link.springer.com/article/10.1007/s10676-016-9394-0

SCHWAB, KLAUS (2016) SHAPING THE FOURTH INDUSTRIAL REVOLUTION, PROJECT SYNDICATE. Disponível em: https://www.project-syndicate.org/commentary/fourth-industrial-revolution-human-development-by-klaus-schwab-2016-01

SOLOVE, DANIEL J. (2004) *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE LNFORMATION AGE*, NEW YORK UNIVERSITY PRESS;

STALLMAN, RICHARD. Richard Stallman's Personal Site at: https://stallman.org/

SZABO, CARL, *IN THE AGE OF EMAIL, ONLINE PRIVACY IN THE AFTERLIFE?,* DAILY JOURNAL, EDIÇÃO DE 9/8/2014, *Reprint version*, disponível em: https://netchoice.org/daily-journal-age-email-online-privacy-afterlife/ ;

TOFFLER, ALVIN (1980) *THE THIRD WAVE*, WILLIAM MORROW AND COMPANY, INC. NEW YORK;

VOGEL, KLAUS (1999) *"THE TRANSPARENT MAN- SOME COMMENTS ON THE HISTORY OF A SYMBOL"*, IN *MANIFESTING MEDICINE: BODIES AND MACHINES*, ED. ROBERT BUD, BERNARD FINN AND HELMUTH TRISCHLER (AMSTERDAM, HARWOOD ACADEMIC PUBLISHERS), pp. 31-61;

***WARREN**, SAMUEL D., **BRANDEIS**, LOUIS D.. THE RIGHT TO PRIVACY.* ORIGINALLY PUBLISHED IN THE *HARVARD LAW REVIEW*, V. IV, NO. 5,

DECEMBER 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm;

WRIGHT, NICOLA (2014) *DEATH ANT THE INTERNET: THE IMPLICATIONS OF THE DIGITAL AFTERLIFE*, *online journal FIRST MONDAY*, VOL. 19, NUMBER 6, disponível em: http://pear.accc.uic.edu/ojs/index.php/fm/article/view/4998/4088#author

ZITTRAIN, JONATHAN (2008) *THE FUTURE OF THE INTERNET AND HOW TO STOP IT,* YALE UNIVERSITY PRESS & PENGUIN UK. Disponível com licença CC 3.0 em: http://futureoftheinternet.org/download/

II – Doutrina Nacional

ASCENSÃO, José de Oliveira

- "*PROPRIEDADE INTELECTUAL E INTERNET"*, in *BIBLIOTECA DIGITAL IUS COMMUNE* - Disponível em: http://www.fd.ulisboa.pt/investigacao/biblioteca-digital-ius-commune/;
- (2002) "*DIREITO INTELECTUAL, EXCLUSIVO E LIBERDADE*", *in REVISTA ESMAFE: ESCOLA DE MAGISTRATURA FEDERAL DA 5ª REGIÃO,* RECIFE, N. 3, pp. 125-145; Disponível em: http://bdjur.stj.jus.br/jspui/handle/2011/27320;
- (2003) *ESTUDOS SOBRE DIREITO DA INTERNET E DA SOCIEDADE DA INFORMAÇÃO*, ALMEDINA: Coimbra;
- **(1999) "***O DIREITO DE AUTOR NO CIBERESPAÇO*" *in REVISTA DA EMERJ, RIO DE JANEIRO,* V.2, N.7, PÁGINAS 21-43. Disponível em: http://bdjur.stj.jus.br/jspui/handle/2011/73949 .

CANOTILHO, Gomes/ **MOREIRA**/Vital (2007) *CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA ANOTADA,* VOLUME I, 4.ª EDIÇÃO, COIMBRA EDITORA: Coimbra;

CANOTILHO, José Joaquim Gomes (2006). "*JUSTIÇA CONSTITUCIONAL E JUSTIÇA PENAL"*, *in Revista Brasileira de Ciências Criminais*, nº 58, São Paulo, pp. 329-344;

CASTRO, CATARINA SARMENTO E

- (2005) *DIREITO DA INFORMÁTICA, PRIVACIDADE E DADOS PESSOAIS*., ALMEDINA: Coimbra;

- (2016) "*DIREITO À INTERNET*", *in Cyberlaw by CIJIC*. Disponível em: http://www.cijic.org/wp-content/uploads/2016/06/DIREITO----INTERNET_Catarina-Sarmento-e-Castro.pdf

CASTRO, Raquel Alexandra Brízida (2016) "*CONSTITUIÇÃO E CIBERESPAÇO: ARGUMENTOS PARA UM "DIREITO CONSTITUCIONAL DO INIMIGO"?" in Cyberlaw by CIJIC*. Disponível em: http://www.cijic.org/wp-content/uploads/2016/01/CONSTITUI----O-E-CIBERESPA--O_ARGUMENTOS-PARA-UM----DIREITO-CONSTITUCIONAL-DO-INIMIGO---.pdf

FARIA, MARIA PAULA RIBEIRO DE (2010) *CONSTITUIÇÃO PORTUGUESA ANOTADA, ANOTAÇÃO AO ARTIGO 35.º*; COORD. JORGE MIRANDA E RUI MEDEIROS, COIMBRA EDITORA.

FIGUEIREDO DIAS, JOSÉ EDUARDO DE (2001) "*DIREITO À INFORMAÇÃO, PROTEÇÃO DA INTIMIDADE E AUTORIDADES ADMINISTRATIVAS INDEPENDENTES", in ESTUDOS EM HOMENAGEM AO PROF. DOUTOR ROGÉRIO SOARES,* STVDIA IVRIDICA 61, AD HONOREM-1, BOLETIM DA FACULDADE DE DIREITO, UNIVERSIDADE DE COIMBRA, COIMBRA EDITORA.

GARCIA, NUNO M. *A IMPORTÂNCIA DA INTERNET LIVRE E ABERTA* (2016) Cyberlaw by CIJIC. Disponível em: http://www.cijic.org/wp-content/uploads/2016/06/A-IMPORT--NCIA-DA-INTERNET-LIVRE-E-ABERTA_Nuno-M-Garcia.pdf

MENEZES LEITÃO, LUÍS MANUEL TELES DE (2011) "*DISPOSITIVOS TECNOLÓGICOS DE PROTECÇÃO E DIREITO DE ACESSO DO PÚBLICO*" (Jul/Set 2011) *in REVISTA DA ORDEM DOS ADVOGADOS.* ANO 71. VOL. III.. PÁGINAS 735-750. Disponível em: http://portal.oa.pt/comunicacao/publicacoes/revista/ano-2011/ano-71-voliii-jul-set-2011/doutrina/ .

MORAIS, CARLOS BLANCO (2014) *CURSO DE DIREITO CONSTITUCIONAL, TOMO II*, COIMBRA EDITORA: Coinmbra;

MOREIRA, TERESA COELHO (2011) "*O CONTROLO ELECTRÓNICO DOS EMAILS DOS TRABALHADORES", in CONGRESSO IBERO AMERICANO DE DERECHO INFORMÁTICO.*

NOVAIS, JORGE REIS. *OS PRINCÍPIOS CONSTITUCIONAIS ESTRUTURANTES DA REPÚBLICA PORTUGUESA*. (2004) COIMBRA EDITORA: COIMBRA.

OTERO, PAULO (2007) *INSTITUIÇÕES POLÍTICAS E CONSTITUCIONAIS*, Volume I, Almedina: Coimbra;

PINHEIRO, ALEXANDRE SOUSA (2015) *PRIVACY E PROTEÇÃO DE DADOS PESSOAIS: A CONSTRUÇÃO DOGMÁTICA DO DIREITO À IDENTIDADE INFORMACIONAL*, LISBOA, AAAFDL.

SANTOS, CRISTINA MÁXIMO DOS (1999) "*AS NOVAS TECNOLOGIAS DE INFORMAÇÃO E O SIGILO DAS TELECOMUNICAÇÕES*", *in REVISTA DO MINISTÉRIO PÚBLICO;*

III – Links Institucionais

AMERICAN CIVIL LIBERTIES UNION (ACLU). https://www.aclu.org/

CIM, THE CHARTERED INSTITUTE OF MARKETING. http://www.cim.co.uk/

CNPD, COMISSÃO NACIONAL PROTECÇÃO DE DADOS. https://www.cnpd.pt/

COMISSÃO DAS COMUNIDADES EUROPEIAS, COM(2007) 228 final, Bruxelas, 2.5.2007 - COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO relativa à promoção da protecção de dados através de tecnologias de

protecção da privacidade, disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52007DC0228&from=en

CONSELHO CONSULTIVO DA GOOGLE PARA O DIREITO A SER ESQUECIDO(A), com vídeos das reuniões públicas dos seus membros em: https://www.google.com/advisorycouncil/

_____, *FINAL REPORT*. (6/2/2015) disponível em: https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view

CREATIVE COMMNONS, https://creativecommons.org/licenses/by/3.0/pt/

ENISA: *ENISA'S POSITION ON THE GENERAL DATA PROTECTION REGULATION (GDPR)* (Jan2016), disponível em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-position-on-the-general-data-protection-regulation-gdpr/

_____, *ONLINE PRIVACY TOOLS FOR THE GENERAL PUBLIC* , disponível em : https://www.enisa.europa.eu/publications/privacy-tools-for-the-general-public .

_____, *PRIVACY AND DATA PROTECTION BY DESIGN*, disponível em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design .

_____, *READINESS ANALYSIS FOR THE ADOPTION AND EVOLUTION OF PRIVACY ENHANCING TECHNOLOGIES METHODOLOGY, PILOT ASSESSMENT, AND CONTINUITY PLAN*, disponível em: https://www.enisa.europa.eu/publications/pets/at_download/fullReport .

EUROPEAN DIGITAL RIGHTS (EDRi) - *THE CHARTER OF DIGITAL RIGHTS* (2014) – disponível em: https://edri.org/wp-content/uploads/2014/06/WePromiseCharter_booklet_web.pdf .

_____, *AN INTRODUCTION TO DATA PROTECTION* (2013), disponível em: https://edri.org/wp-content/uploads/2013/10/paper06_web_20130128.pdf .

_____, *YOUR GUIDE TO THE DIGITAL DEFENDERS (KIDS BOOKLET* – (2016), disponível em: https://edri.org/files/privacy4kids_booklet_web.pdf

IACA - THE INTERNATIONAL ANTI CRIME ACADEMY . Open Source Intelligence and Social Media Intelligence. Disponível em: http://www.anti-crime-academy.eu/

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP) - https://iapp.org/

OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA,
(v. C(80)58/FINAL) disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm e,
(v. amended on 11 July 2013 by C(2013)79), disponível em: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

PRIVACY BRIDGES: *EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS*. (September 2015), INSTITUTE FOR INFORMATION LAW (IVIR) UNIVERSITY OF AMSTERDAM/ MASSACHUSETTS INSTITUTE FOR TECHNOLOGY COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY (CAMBRIDGE, MA – UNITED STATES), Relatório disponibilizado no âmbito *do 2015 International Conference of Privacy and Data Protection Commissioners*, disponível em: https://privacybridges.mit.edu/

PROFILING PROJECT. THE RIGHT OF DATA PROTECTION IN THE CONTEXT OF PROFILING. http://profiling-project.eu/

_____, **DEFINING PROFILING**: FIRST PAPER OF PROFILING PROJECT (2013), V. FERRARIS (AMAPOLA); F. BOSCO, G. CAFIERO, E. D'ANGELO, Y. SULOYEVA (UNICRI), AND INTERNAL REVIEWER: B.J. KOOPS. Disponível em: http://profiling-project.eu/defining-profiling-first-paper-of-profiling-project-online/ .

_____, **PROTECTING CITIZENS' RIGHTS FIGHTING ILLICIT PROFILING** (2014). FINAL REPORT OF THE PROFILING PROJECT UNDER SCIENTIFIC COORDINATION OF BERT-JAAP KOOPS (Tilburg Institute for Law, Technology and Society – TILT) Disponível em. http://profiling-project.eu/final-report-of-the-profiling-project/ .

SOCIAL SCIENCE RESEARCH NETWORK ("SSRN"). Em: https://www.ssrn.com/en/;

UNIÃO EUROPEIA, AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. *MANUAL DA LEGISLAÇÃO EUROPEIA SOBRE PROTEÇÃO DE DADOS / FRA — AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA*, (2014) versão portuguesa disponível em: http://www.infoeuropa.eurocid.pt/registo/000066668/

UNITED NATIONS HUMAN RIGHTS COUNCIL (UNHRC). *THE PROMOTION, PROTECTION AND ENJOYMENT OF HUMAN RIGHTS ON THE INTERNET*. (2016) 32ND SESSION, 30 DE JUNHO. http://www.ohchr.org/EN/Pages/Home.aspx

WEBFOUNDATION.ORG

*IV – **Legislação***

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2010/C 83/02), disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:PT:PDF

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA (actual). Disponível em: http://www.tribunalconstitucional.pt/tc/crp.html .
CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA (versão originária). Disponível em: http://www.tribunalconstitucional.pt/tc/content/files/crp/crp1976.pdf

CONVENÇÃO 108 PARA A PROTECÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS, de 28 de janeiro de 1981

DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 24 de Outubro de 1995, directiva de protecção de dados, *v.g.*, DPD., disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046 .

TRATADO DA UNIÃO EUROPEIA (VERSÃO CONSOLIDADA), disponível em: http://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679

NOTA: As notícias e artigos de opinião, de jornais e revistas, seguem nas notas de rodapé com os respectivos *links* e data de último acesso.