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[1]. 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 –

[1] 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[2], 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

[2] 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*[3] 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*[4] 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[5] - concepts such as privacy

3 As Lawrence Lessig posed it.

4 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.

5 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[6], 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.

6 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[7]. 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*[8]*»*, 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

---

7 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.

8Available (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[9] , 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

9 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*[10], 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

10As 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[11], 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[12] 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?

[11] The Law, is the *older* 2007 version of the Law on access to administrative documents (in Portuguese, L.A.D.A).
[12] 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.