
CYBERLAW
by CIJIC

EDIÇÃO N.º V – MARÇO DE 2018

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Antes de mais, salientarei uma novidade interna na organização do CIJIC. Desde final de Fevereiro de 2018, depois da assembleia geral, o Centro, passou a estar organizado, sob a Presidência do Professor Doutor Eduardo Vera-Cruz Pinto, coadjuvado por duas Vices, respetivamente, as Professoras Doutoras, Paula Vaz Freire e Raquel Alexandra Brízida Castro, e pelos vogais, Eugénio Alves da Silva e Nuno Teixeira Castro. Mais novidades surgirão em breve.

Feito o ponto de ordem inicial, e abertas as hostilidades, nesta nova edição, sem descurar a proximidade da entrada em vigor, em pleno, do *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),* doravante, no acrónimo, RGPD, optamos por trazer a debate algumas tendências de futuro. Obviamente, quase todas com implicações, pungentes, quer ante o instrumento legislativo europeu em foco, quer, e acima de tudo, ante as formas mais tradicionais de relacionamento interpessoal e em sociedade.

Antecipando a tónica, o nosso futuro, já hoje muito intrincado com o digital, dependerá, no seu essencial, da contínua promoção de princípios e valores humanos que, ao longo dos tempos, nos foram acompanhando na evolução enquanto espécie racional. A compreensão, teoricamente mais facilitada até pelo dilúvio informacional

do presente, do conceito, *jus cogens*, de dignidade humana, deveria possibilitar a criação de uma consciência, atrever-nos-íamos a estribar de colectiva, global, do valor individual de cada vida humana em si considerada. Deveria. Porém, pouco disto tem vindo a suceder. As informações e notícias diárias têm vindo a sustentar precisamente um movimento díspar: uma sociedade hedonista mas profundamente egoísta, enamorada por um *surveillance capitalism*[1] reinante, sem espaço para a promoção da fundamentalidade de cada individualidade humana.

O poder inebriante, e sem precedentes na nossa história civilizacional, detido por algumas organizações, denominadas de *tech-giants*, tem rompido as estruturas sociais, políticas, comerciais e, até, tecnológicas. Qual a origem de tão avassalador poder disruptivo destas organizações, destes *tech-giants*?

Em parte, grande, o *graal* destes *tech-giants* deriva de todo o *dilúvio informacional* que percorre a rede. Numa relação de *win-win*, a "*oferta inocente"* de serviços, prosaicamente assimilados como *grátis*, em troca dos nossos dados pessoais, é obnóxia para o indivíduo. Mas profundamente fluída no garante de volumosos acréscimos de capital financeiro, e por conseguinte, de poder, para estas organizações. Bruce SCHNEIER[2], a este propósito, sintetiza de forma lapidar: «*Companies like Facebook and Google offer you free services in exchange for your data. Google's surveillance isn't in the news, but it's startlingly intimate. We never lie to our search engines. Our interests and curiosities, hopes and fears, desires and sexual proclivities, are all collected and saved. Add to that the websites we visit that Google tracks through its advertising network, our Gmail accounts, our movements via Google Maps, and what it can collect from our smartphones. That phone is probably the most intimate surveillance device ever invented. It tracks our location continuously, so it knows where we live, where we work, and where we spend our time. It's the first and last thing we check in a day, so it knows when we wake up and when we go to sleep. We all have one, so it knows who we sleep with.*» Sim, *o smartphone é provavelmente o dispositivo, mais íntimo,* pessoalíssimo mesmo, *de vigilância jamais inventado.* Acompanha-nos permanentemente, 24h/7d, 365d/ano, qual extensão do nosso corpo. E sempre a debitar

1 https://www.amazon.com/Age-Surveillance-Capitalism-Future-Frontier/dp/1610395697
2 https://www.schneier.com/

informação para alguém, transformando-nos no escravo, informacional, do...objecto. Curioso, não?

De facto, disfarçado de *pot-pourri* de intimidade, proximidade e confiança cega, os gigantes tecnológicos têm-nos orientado a um estado de, *quase-completa,* submissão a variadíssimas formas de engenharia social, perfumada por formas competentes e persuasivas de direcção comportamental, categoricamente personalizadas e orientadas para fazermos *algo ao serviço de alguém*; uma verdadeira manipulação individualizada orientada pelo perfil de cada um, de previsão e controlo do nosso comportamento. Fácil de conseguir quando em posse de tão valiosa informação que vamos cedendo, sem limites. Sem conhecimento. Sem oposição. Shoshana ZUBOFF[3] arroja duas questões sufocantes, a cada um de nós, nesta era digital da sociedade informacional: "*Mestre ou escravo*?", "*Casa ou exílio*?". (Conseguiremos responder?)

Os desafios para o futuro da humanidade travam-se. Fugir, ou recear tal, não poderá ser a resposta. Nesta conjuntura crítica, nesta *nova fronteira do poder*, o confronto entre o, vasto, poder dos gigantes tecnológicos versus os dos governos (enquanto representantes da nossa comunidade colectiva), atira-nos, sem pudor, para um difícil campo de escolhas, civilizacionais diria. O futuro da humanidade tem espaço para a autonomia individual e para os direitos fundamentais? Ou assistiremos impávidos ao desabrochar de novas e sofisticadas formas de desigualdade social? O *el dorado* da era digital possibilitará o fortalecimento dos direitos fundamentais individuais e a sua democratização globalizante? Ou assistiremos impávidos à instrumentalização do indivíduo, segmentado em objecto de informações em meras *strings de bits*, coisificado, servil ao *surveillance capitalism*?

Nesta insolência de questões, e uma vez aqui chegados, foi nossa intenção suscitar a comunidade académica e empresarial a problematizar algumas teorias de resposta. Não assumindo o absolutismo das coisas, o resultado presente é, a nosso ver, profundamente satisfatório. Neste nosso *pot-pourri* que agora publicamos, carreamos *big data*; segurança da informação; regulamento geral de protecção de dados; veículos autónomos e inteligentes; *criptocontratação*; contratos automatizados e contratos

3 http://www.shoshanazuboff.com/

inteligentes; dados pessoais e direitos fundamentais; e, mecanismos de cooperação e coerência no tratamento de dados pessoais.

Agradecidos pelo esforço e pelo trabalho, cumpre-me, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, endereçar um especial reconhecimento a cada um dos autores.

Um sentido e imenso Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 30 de Março de 2018

Nuno Teixeira Castro

DOUTRINA

WE ARE BIG DATA: NEW TECHNOLOGIES AND PERSONAL DATA MANAGEMENT

EDUARDO MAGRANI *

&

RENAN MEDEIROS DE OLIVEIRA *

* Ph.D. and Coordinator of the Institute for Technology and Society of Rio de Janeiro (ITS Rio). Contacto: eduardomagrani@gmail.com
* Researcher at FGV DIREITO RIO. Contacto: renanmedeirosdeoliveira@gmail.com

RESUMO

Este artigo almeja apresentar, num presente de hiperconectividade, uma visão crítica quanto à utilização de dados pessoais, propondo, em alternativa e com base num projecto concreto, um cenário de resposta de dados de autogestão. Primeiramente, debruçar-nos-emos sobre o quadro da privacidade no Século XXI, procurando enfatizar de que estamos na presença de um direito multifacetado, que ganhou novos contornos diante das tecnologias contemporâneas e que apresenta uma série de desafios que ainda não obtiveram resposta. Em segundo lugar, introduziremos a noção de big data, conceito que reporta qualquer quantidade volumosa de dados estruturados, semi-estruturados ou não estruturados, e que apresente o potencial de vir a ser explorado para obter informações. Procuraremos destacar, ainda, que a noção de big data também se reporta a todos nós, às nossas informações, e que não nos faltam incentivos para recuperar o controlo sobre tais informações. Num terceiro momento, vamos procurar contextualizar o projeto de gestão de dados pessoais chamado MyData. Finalmente, concluiremos a nossa análise argumentando que um projeto assim pode ser uma alternativa eficaz para proteger o direito à privacidade neste mundo contemporâneo.

***Palavras-Chave**: Privacidade, Big data; gestão de dados; Internet das coisas*

ABSTRACT

This article aims to present a critical view on the use of personal data in the current scenario of hyperconnectivity, bringing to the fore, as an alternative, the possibility of self-managing data, based on a concrete project. We will first present a panorama of privacy in the twenty-first century emphasizing that it is a multifaceted right that has gained new contours in the face of contemporary technologies and presents challenges that have not yet been answered. Second, we will introduce the notion of big data, a term that describes any voluminous amount of structured, semi-structured or unstructured data that has the potential to be exploited to obtain information. We will also try to highlight the notion that the big data is us and that we have incentives to regain control over this information. In a third moment, we will give an exposition about the personal data management project called MyData. We will conclude this analysis by arguing that a project of this kind can be an effective alternative to protect the right to privacy in the contemporary world.

Keywords: Privacy, Big Data, Data Management, Internet of Things.

1. INTRODUCTION

Technology has advanced rapidly and contributed to improve the way we live. In addition to interfering with how individuals act, it changes the way people relate to each other, to business, and to government. The many changes emphasize the need to give importance to the individual and to have a multisectoral dynamics to build a sustainable Internet governance. It is undeniable that new technologies bring benefits. However, there are regulatory and ethical questions related to their use. With more and more connected devices, related to the scenario that has been called Internet of Things (IoT)[1], there are several risks and challenges, such as those related to the right to privacy.

Data generated through the use of these numerous smart devices are collected and stored by companies, which do not always act transparently. Terms of use and service are often extremely technical and unintelligible to the general population. It is not uncommon that the intended purpose of the data be hidden from the users themselves, who have no control over the information that refers to them. Given the voluminous amount of data produced daily, this becomes even more worrisome, especially since the "Big Data" phenomenon goes far beyond a tangle of data, being essentially relational. We must bear in mind that Big Data is us, and therefore we must have a critical conscience about it and think about possibilities to regain control over our personal data.

With ownership and availability of our data, companies use techniques such as targeting, tracking, and profiling to target their marketing policies to the way we live and our needs - or to what they make us believe to be a necessity. In this way, discussions about the right to privacy are inextricably linked to discussions about the use and management of data. The technological advance requires adaptations of the legal order to the new scenarios, which can

1 In general, the Internet of Things can be understood as an ecosystem of physical objects interconnected with the Internet, through small embedded sensors, creating a ubiquitous computing ecosystem, aimed at facilitating everyday people, introducing functional solutions to day-to-day processes.

happen, for example, through the legislative action or the interpretive activity. These solutions are not always effective: on the one hand, the sociopolitical conjuncture and the technological pattern change much more rapidly than legislation can accompany, and, on the other hand, paternalistic and corporative distance from the will of individuals. Thus, new ways to protect the right to privacy and to increase the control that Internet users have about their own data have emerged as an alternative.

In this sense, the MyData project was created. It is basically a system whose objective is to place the individual at the center of personal data so that they themselves have control of the information produced about themselves, being free from the abusive control of data currently exercised by companies. It adopts a perspective centered on the human being, and no longer on the things or the information itself. In the current management model, the data is from those who collect it. Individuals to whom the information refers to, do not even know in general the purpose for which they are used, which creates serious privacy problems and fails to meet the principle of transparency. The new system seeks to create a scenario in which users have their human rights respected in the digital environment and can control their data while creating barriers to business innovation that can develop based on mutual trust.

The present study aims to analyze this project in a more detailed way and seeks to highlight the benefits it can bring to the protection of privacy and the taking of control over personal data by the individuals themselves. To do this, we will first present a brief overview about the right to privacy, its contours and the impact of new technologies. In a second moment, aspects related to Big Data will be analyzed, so that a more delineated notion about the production and storage of data is made. Third, we will present in more detail the personal data management project mentioned above. We conclude with an analysis of how this project tends to contribute to the protection of privacy in the context of new technologies.

2. THE CHALLENGE OF PRIVACY IN THE HYPERCONNECTED WORLD

The protection of privacy is a fundamental point of societies that are intended to be democratic and is envisaged as a fundamental right in the American Convention on Human Rights (article 11) and in the Universal Declaration of Human Rights (article 12). International treaties on the subject generally deal with privacy in the face of non-interference in family private life, correspondence and communications, as does the Brazilian Federal Constitution of 1988[2]. The interpretation of privacy, however, has been changing substantially in recent years and this right has gained new contours.

The right to privacy consists of a complex value [44] having different meanings and different aspects that characterize it. Among these aspects, we have the traditional view of the right to be left alone [57], which implies control by the individual on information that relates to his or her personal life. [53] The right to privacy involves the right to prevent strangers from accessing information about privacy and not disclosing it. [53] There is also the one which deals with the right to privacy from the perspective of protection with other interferences - which implies the individual's right to be left alone in order to live his life with a minimum degree of interference -, from the point of view of the secrecy of certain information and, finally, from the point of view of control over information and personal data [26].

With social and technological development, different facets of privacy emerge, and new conflicts and problems erupted [55] [28], such as the debate about the right not to become aware of personal data [36], the discussion on non-authorized biographies [35] and the "right to non-tracking" [30]. In the information society, privacy must be understood in a functional way, in order

2 In Brazil, the right to privacy, a sphere of the right to privacy, is intimately connected with the protection of human dignity and personality and can be derived from the constitutional recognition given to intimacy, privacy and the inviolability of data [53]. We highlight the following provisions of the Federal Constitution on the topic: art. 5 (...) X - "the privacy, private life, honor and image of persons shall be inviolable, ensuring the right to compensation for material or moral damages resulting from their violation;" and XII - " correspondence, telegraphic communications, data and telephone communications secrecy is inviolable and, except in the latter case, by court order, in the cases and in the form established by law for the purposes of criminal investigation or criminal proceedings;".

to assure a subject the possibility of "knowing, controlling, addressing, or interrupting the flow of information related to it" [48]. Accordingly, Stefano Rodotà [48] defines privacy "as the right to maintain control over the information itself".

There is no final concept for the right to privacy and the notion of private life has been expanded due, among other factors, to the development of technology. The technological factor has a prominent role, since with the improvement of the layer of information storage and communication, new ways of organizing, using and appropriating information arise. Technological development allows for the creation of behavior profiles that can even be confused with the person [15]. Such profiles, combined with the manipulation of data collected, can generate serious impacts on freedom: "*Another technique still concerns a data collecting modality, known as data mining. It consists in the search for correlations, recurrences, forms, trends and significant patterns from very large amounts of data, with the aid of statistical and mathematical instruments. Thus, from a large amount of raw and unclassified information, information of potential interest can be identified*" [15].

Thus, while, on the one hand, technology brings undeniable benefits to society, it creates, on the other hand, problems for privacy protection. Although technology helps to shape a richer private sphere, it contributes to the increasingly fragile and threatened sphere, which gives rise to the need to continually strengthen its protection [48]. The need for greater protection of personal data goes deep into the Internet of Things scenario. In this context, increasing connectivity with the most diverse technology devices generates a virtually inexhaustible source of information about the day-to-day of users of such devices. Considering that when we speak in private we have personal information in mind [50], it is essential to devote special protection to the data and information generated through Internet connections and devices connected to IoT.

Brazil, unlike most countries in Latin America [3] and Europe [3] [45], does not yet have a sufficient legislative framework to guarantee the protection

of privacy at all times[3]. There are bills currently in progress at the National Congress seeking to pass a general law on privacy and personal data protection[4]. However, protection should not only be governed by legislation, since laws are limited in time due to rapid social change. Thus, considering that privacy should also be understood as positive freedom, it is fundamental to create mechanisms that give individuals the power to control their own data, the processes to which they will be subjected to and the purposes underlying their use. One of the possible alternatives for protecting privacy and empowering individuals to control their data is personal data management, which will be presented in more detail below.

3. WE ARE BIG DATA: BETWEEN ECONOMIC EXPLOITATION AND PERSONAL DATA CONTROL

Every day, we connect to the Internet through devices that have the ability to share, process, store, and analyze a huge amount of data. This situation generates what we know as Big Data, which is an evolving term that describes any voluminous amount of structured, semi-structured or unstructured data that has the potential to be exploited for information[5] [25].

3 The Brazilian Constitution provides for recognition of the right to privacy, privacy (article 5, X) and inviolability of data (article 5, XII), and points to habeas data as an instrument capable of ensuring the protection of information and personal data (Article 5, LXXII). There is also legislative protection at the infra-constitutional level. The Civil Code of 2002 protects private life (article 21) and the Consumer Protection Code devotes Section VI to the protection of databases and consumer registries. Lastly, the Civil Internet Framework, in force since 2014, covers the protection of privacy and data as principles to be observed in the Internet discipline as a pillar of the Law (article 3, subsections II and III). Articles 7 and 10 of the Civil Code also address the issue. Such regulation, however, is insufficient to protect personal data and privacy in its many facets.

4 Between the years 2013 and 2014, bills 330/2013, 181/2014 and 131/2014 were proposed, which had on the protection of personal data in general and the provision of data of Brazilian citizens and / or companies to foreign bodies, fruits of the Espionage CPI carried out by the Federal Senate. By 2015, these three projects have been scrapped and are being handled today. Also jointly process bill 4060/2012 and Draft 5276/2016. Project No. 5276/2016 provides important principles for effective protection of privacy and personal data, such as the principle of finality, the principle of adequacy and the principle of necessity. The bill was heavily influenced by European regulation, with many similarities to the General Data Protection Regulation of 2016.

5 For José Carlos Cavalcanti, the Big Data concept applies to information that cannot be processed or analyzed using traditional processes or tools. Cavalcanti mentions as basic characteristics of the

The first property involving Big Data consists of the increasing volume of data [47]. A recent survey by Cisco [9] estimates that over the next few years the measure in gigabytes (1 trillion bytes) will be exceeded and the amount of data will be calculated in the order zettabyte (10^{21} bytes) and even in yottabyte (10^{24} bytes).

Another property involves the high speed [9] with which data is produced, analyzed and visualized. In addition, the variety of data formats represents an additional challenge. This feature is enhanced by the different devices responsible for collecting and producing data in different environments. The information provided by a mechanism that monitors the temperature is quite different from that obtained in social networks, for example. In addition, most of the data found is not structured [9] [34].

The concept of Big Data may also imply, together with the concept of Data Science, the ability to transform raw data into graphs and tables that allow an understanding of the phenomenon to be demonstrated. It is important to mention that, in a context where decisions are increasingly made on the basis of data, it is extremely important to ensure the accuracy of this information [32]. Although this is not a new phenomenon, "what the Internet did was to take a new dimension, transforming it. To understand these transformations, we need to understand that Big Data is us" [52].

The combination of intelligent objects and Big Data can significantly change the way we live [19]. Research [4] estimates that by 2020 the number of interconnected objects will increase from 25 billion to 50 billion intelligent devices. Projections for the impact of this hyperconnection scenario on the economy are impressive, corresponding globally to more than $11 trillion in 2025 [51].

Intelligent and interconnected objects can effectively help us in solving real problems. From the point of view of consumers, the products that today

Big Data concept: volume, variety and velocity (the so-called 3 Vs, concept previously created), also recognizing "truthfulness" as another possible characteristic defended by other authors [7]. The 3 Vs have been used by the doctrine to refer to Big Data since mid-2010 [20].

are integrated with the technology of the Internet of things come from the most varied areas and they have diverse functions, from electrical appliances, means of transport to toys. There are also pieces of clothing that have IoT connectivity, being part of a category called wearables. These wearable technologies consist of devices that are connected to each other producing information about the users and the people around them. Among the main products are the bracelets and sneakers that monitor the physical activity of the user, as well as clocks and smart glasses that intend to provide the user with an experience of immersion in the reality itself [24] [12] [38].

However, transforming an analog object into an intelligent one, in addition to making the product expensive and subject to flaws that it would not have a priori, can also create risks in relation to security and privacy [50]. We are talking about a context that involves a massive volume of data being processed, on the scale of billions of data daily, allowing it to be possible to know more and more individuals in their habits, preferences, desires and thus trying to direct their choices. This need has been well explored by the market, which has explored the possibility of personalization and automatic customization of content on digital platforms, including capitalizing on filtering with targeted advertising through cookie tracking and retargeting processes or programmatic (behavioral) media retargeting [40]. There is now no clear treatment of the data [2]. Aspects about the collection, sharing and potential use of them by third parties are still unknown to consumers. This has the power to shake - and, in a sense, already shakes [8] [11] [2] [42] - users' confidence in connected products [33].

It should also be noted that security holes open space for attacks aimed at accessing the information generated by the devices themselves. In addition, intelligent devices, when invaded, can generate problems not only for the device itself, but also interfere with the network infrastructure itself [10]. Issues related to security and protection of personal data are equally important for IoT to consolidate as the next step on the Internet.

Given this scenario, one of the most important issues related to the protection of personal data is who controls them and who has access to them.

In the current model, technology companies are endowed with this control and have such access. The individual in relation to whom the information is collected often is not even aware that his data is being stored and, when he does know, it is not uncommon that he is unaware of the purpose of such collection and storage. A society that aims at being transparent and democratic cannot dispense of clear and fair forms of data management. It is necessary to equip individuals with control of their own data and to empower them to decide what, with whom, when and why to share.

4. PERSONAL DATA MANAGEMENT PROJECT

Online interaction is constant and is present in the lives of almost all individuals. In the hyperconnected contemporary world, information and news gathering is increasingly occurring through the Internet, as is the contracting of products and services, which increasingly occur digitally, as well as the establishment of social and professional contact through social networks. This, however, often goes unnoticed by users, who do not realize the digital traces they produce about themselves. The data produced, not infrequently, is stored for a long period of time. The control of this trail has become a technological and social problem, since from its analysis it is possible to obtain information about the behavior, preferences and personal needs of a certain person and even to predict their future actions.

An example of predicting people's future actions based on their buying habits, which demonstrates the danger of free use of personal information, is the cross-referencing of data made by sales companies. Target creates an identity of each consumer through information obtained when the customer uses the credit card, a promotional coupon, contact the SAC or visit the online store. The company realized that if a woman buys some items together or in larger quantities, such as unscented lotions, coconut butter lotions, zinc and magnesium supplements, and a large purse, there is an 87 percent chance she

is three months pregnant [49] [46]. An interesting case occurred in 2012, when the company delivered discount coupons to a woman, but her father received them instead, receiving the surprising news that his daughter was pregnant [16].

Despite this collection of Big Data about individuals and the formation of individual profiles, individuals do not usually have access to the personal data about them generated. Large Internet companies, such as Google and Facebook, centralize the collected information and encourage people to use only their tools, since there is no sharing of information between them, which is in line with the competition in the market and the innovation. The user does not control his personal data [54]. One of the recently proposed technical solutions to this problem points to personal data centered on the human being, that is, individuals themselves should control their data.

Personal data has an increasingly significant social, economic and practical value, but its application and wider use is often confused with negative predictions of a future devoid of individual privacy. MyData consists of a human-centered (other than the current organizational system) and rights-based framework for data management. Individuals must be at the heart of their own data control and their digital human rights must be strengthened while companies are able to develop innovative services based on mutual trust. [43] MyData allows the collection and use of personal data in order to maximize the benefits obtained while minimizing lost privacy. Thus, these valuable data will enable individuals to interact with vendors, who can offer better data and consumer services [43].

This MyData-based, interoperable infrastructure approach provides individuals with data-based services with greater privacy and transparency, which enhances freedom of choice both empowering and benefitting the individual. Consent management is the main mechanism for enabling and enforcing the legal use of data. In this model, consents are dynamic, easy to understand, machine-readable, paired and coordinated. A common format will allow each individual to delegate the processing of data to third parties or reuse the use of data in new ways [43].

MyData equips individuals to control who uses their personal data, estimating what purposes may be used and giving informed consent in accordance with personal data protection regulations. Data flows become more transparent, comprehensive and manageable. Users can also turn off information flows and withdraw consent. Finally, machine readable consents can be viewed, compared and processed automatically [43].

In addition, MyData can be considered useful to companies because it will help integrate complementary third-party services into their core services; will simplify operations within current and future regulatory frameworks and allow the use of data for exploratory purposes; and will enable the creation of new business based on data processing and management [43].

It's interesting to note that MyData is complementary to Big Data, and vice versa, because without addressing the human perspective, many of Big Data's' innovative potential uses are incompatible with the regulations currently in place.

This approach has three principles that require maturation: **(i) control over data centered on the human being**: the human being is an active actor in managing his / her life online and offline and "has the right to access his / her personal data and control his / her privacy settings" [5] as much as is necessary to make them effective; **(ii) usable data**: personal data must be technically easy to access and readable by Application Programming Interfaces (APIs). MyData converts data into a reusable resource to create services that help individuals manage their lives; **(iii) open business environment**: infrastructure enables the de-centralized management of personal data, enhances interoperability, facilitates compliance of companies with data protection regulations, and enables individuals to switch service providers without data blocking. Thus, "by meeting a common set of personal data standards, businesses and services allow people to exercise freedom of choice between interoperable services," preventing people from having their data locked into "per- only one company because they cannot export them" and take them to another provider [5].

MyData is a more robust infrastructure than simple APIs. The data aggregator being used today is naturally evolving out of the API economy, but it has significant disadvantages: the lack of interoperability between data aggregators and the fact that the current source of aggregators does not necessarily recognize privacy or engages in a transparent relationship with individuals. Adopting the MyData approach can lead to a systemic simplification of the personal data ecosystem, and this simplification can be done gradually, as the platform can be developed and deployed in stages, alongside the evolution of the API economy and the model of data aggregator [43].

Finally, it is interesting to see how the MyData architecture works, which is based on interoperable, standardized accounts: "The model provides individuals with an easy way to control their personal data from a single place, even if data is created, stored, and hundreds of different services. For developers, the model facilitates data access and removes dependency on specific data aggregators. Accounts will usually be provided by organizations that act as MyData operators. For organizations or individuals willing to be operator-independent, it will also be technically possible to host individual accounts, just as some people currently choose to host their own e-mail servers "[43].

The interoperability is the main advantage provided by MyData, but it is also the main challenge because it requires more standardization, more reliable networks and data formats. In the MyData architecture, data flows from a data source to a service or application. The main function of a MyData account is to enable consent management. APIs allow interaction between data sources and users [43]. As already mentioned, the standardized architecture makes the accounts interoperable and allows individuals to switch easily from operators.

5. FINAL CONSIDERATIONS: PERSONAL DATA MANAGEMENT AS AN ALTERNATIVE TO PROTECT PRIVACY

The current model by which personal data are managed goes against the right to privacy and transparency, reducing the power of individual choice. The terms of use of online services offered by companies are long enough to discourage users from reading and have technical terms that are not intelligible to the population without specific technological knowledge [5]. The same goes for privacy policies.

Research conducted in 2017 [39] involving 543 participants, showed that 74% of users do not read privacy policies and those who do, spend an average of only 74 seconds on this task. The average time taken to read the terms of service is 51 seconds. For McDonald and Cranor [31], privacy policy reading time is a form of payment. Reading all policies would take 201 hours a year and would be $3,534 per year for each American user. From a national perspective, reading these policies would mean that the time spent would be about $781 billion per year.

People are unaware of the value of their data and, most of the time, do not want to deal with the complication of managing them [13]. As a result, companies use the data in the form they find most interesting, which may involve the sale and transfer of information to third parties, increasing the risk of leakage and thus privacy breach. The fact that data are non-rivals, that is, they can be used at the same time by more than one person or algorithm, creates complications, such as to give them a different destination from the one to which the user has expressed consent. In this scenario, the data belongs to those who collect them, not the person they refer to.

Researchers at the Getulio Vargas Foundation's Technology and Society Center conducted a study comparing 50 terms of use and service from online platforms analyzing how they deal with the rights to freedom of expression, privacy and due process. The authors concluded that, under this view, the terms

are deficient. The main objective of companies who adopt them is to "minimize exposure to liability, rather than detail their obligation to ensure respect for certain rights," [56] which explains both the vague and ambiguous terminology applied and the tendency for users to have access to as little information as possible, particularly on issues crucial to the protection of human rights "[56]. The study showed, for example, that 62% of companies have clauses requiring users' consent for the sharing of data for commercial purposes [56], which leads us to question whether the consent given by the user is effectively informed.

Issues of privacy and data management on the part of companies lead us to understand that the currently existing consent model has failed. By this model, personal data has become a currency that can be used by individuals to access content online. In other words, to enjoy a service and not be excluded from its use, the individual consents to the access, processing and disclosure of personal data [5].

The ineffectiveness of the terms of service and the lack of informed consent are even clearer in the Internet of Things. Unisys 2017 Research Security involved citizens from 13 countries and showed that Brazilians are most willing to provide their personal data in return for the convenience of connectivity between their devices. As an example, 88% of Brazilians are in favor of placing sensors in their luggage to communicate with the airport system and have their items located more easily; 83% accept that health information obtained through pacemakers, among other devices, is shared with physicians; and 50% agree to provide health insurance companies with information related to the physical activities of watches.

The great interest of companies in personal data is mainly due to their economic utility, so that in the present century they are equivalent to what oil meant in the last century [41] [23] [22] [13]. In addition, the data is transported to thousands of computers that extract certain values, such as patterns, predictions and other insights into individuals' digital information - which can be used in marketing policies and artificial intelligence mechanisms." [13]. Digital information comes from different sources and is extracted, refined, valued, bought and sold in different ways. This changes the rules of the market

and demands a new regulatory approach [13]. Individuals must have control over their data and be aware of the fate that will be given to them after authorization for use, which, among other benefits, will increase users' freedom of choice and empower them. Moreover, it is necessary to face the challenge of getting people to understand the value of their data and that they are entitled to compensation for the granting of information [13].

User confidence in the regulation of privacy and freedom of information is intimately connected to democracy [14], and the digital economy is dependent on that trust. Privacy and innovation do not have to be different. The task of developing an infrastructure in which these two elements converge is difficult and requires high levels of dedication. However, the task, which is not impossible, is essential: privacy demands the highest level of innovation [8]. It is necessary that privacy and innovation move together, so that they do not clash and that one does not disturb the evolution of the other. They can and should go in parallel, and this is what the public expects and what the Law demands [14].

In view of these changing needs, the above project has been developed to give the individual the power over their information and to make them the owners of their data - not the companies that collect them. Projects of this bias may be the solution to overcome an Internet dominated by oligopolies, profiling techniques and generalized surveillance [1].

The MyData project starts from the current context of data management, which is harmful to privacy and transparency, and seeks to empower individuals by giving them control over their own data. We are in constant digital interaction and leave traces with every click that we make. Most of these interactions are stored for a long time, which creates a digital history of people and allows you to analyze their behaviors, preferences, needs and even predict future actions. In general, this data is not available to the users themselves and they do not even know what information is being collected and stored. Individuals do not control their own data - companies do. Therefore, the project aims to get people to control their data and decide, based on clear information

and the useful organization of their data if they want to hire a particular product or service.

The system being developed has its central vision focused on being human, but it is also useful to companies, which can create products and services more profitable to the individuals. One point that also deserves mention is the fact that the project is not limited to proposing a data meeting in a single place but presents a model through which individuals can understand and organize their data, in order to obtain the information contained in the systems. However, adherence to this approach is still embryonic. Big companies connected to technology and data management, such as Facebook and Google, are not interested in advancing projects like this, as this is extremely disruptive to their business models. Faced with this, along with the greater dissemination of this type of project, it is necessary to think of ways to make users aware of the value and importance of their data and to know that they can have control over them, defining who will use them, when and for what.

The Internet has given a new dimension to personal information and privacy and has generated what we know as Big Data, which goes far beyond innocuous data: Big Data is us. It is from the recognition of the importance of our data and the development of safe projects that give the individual control over their information that we can ensure effective protection of privacy concerning new technologies.

REFERENCES

1. Abiteboul, S., André, B., & Kaplan, D. Managing your digital life. Communications of the ACM, 58(5), 32-35 (2015, May).
2. Accenture. Digital trust in the IoT era ([s.d.]), www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf, last accessed 2018/02/10
3. Banisar, D. National Comprehensive Data Protection/Privacy Laws and Bills 2016. ARTICLE 19: Global Campaign for Free Expression (2016), https://ssrn.com/abstract=1951416, last accessed 2018/02/18
4. Barker, C. 25 billion connected devices by 2020 to build the Internet of Things. ZDNet (2014, November 11), www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/, last accessed 2018/02/06
5. Belli, L., Schwartz, M., & Louzada, L. Selling your soul while negotiating the conditions: from notice and consent to data control by design. Health Technology (2017), https://link.springer.com/article/10.1007/s12553-017-0185-3, last accessed 2018/01/18
6. Bolton, D. 100% of reported vulnerabilities in the Internet of Things are Avoidable. Applause (2016, September), https://arc.applause.com/2016/09/12/internet-of-things-security-privacy/, last accessed 2018/02/01
7. Cavalcanti, J. The new ABC of ICTs (analytics + Big Data + cloud computing): a complex tradeoff between IT and CT costs. In: J. Martins, & A. Molnar (Org.). Handbook of research on innovation in information retrieval, analysis and management. IGI Global, Hershey, United States (2016).
8. Cavoukian, A. Privacy by Design. IEEE Technology and Society Magazine (2012).
9. Cisco. The zettabyte era: trends and analysis. Cisco (2016, June), www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-

networking-index-vni/vni-hyperconnectivity-wp.html, last accessed 2017/11/19

10. Cobb, S. 10 things to know about the October 21 DDoS attacks. We Live Security (2016, October 24), www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/, last accessed 2017/11/20
11. Consumer Technology Association. Internet of things: a framework for the next administration (white paper) (2016), www.cta.tech/cta/media/policyImages/policyPDFs/CTA-Internet-of-Things-A-Framework-for-the-Next-Administration.pdf, last accessed 2018/02/18
12. Darmour, J. The Internet of you: when wearable tech and the Internet of things collide. Artefact Group ([s.d.]), www.artefactgroup.com/articles/the-internet-of-you-when-wearable-tech-and-the-internet-of-things-collide/, last accessed 2017/12/10
13. DATA IS GIVING rise to a new economy. Economist (2017, May 6), https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy, last accessed 2017/12/10
14. Denham, E. Promoting privacy with innovation within the law (Speech). In 30TH ANNUAL CONFERENCE OF PRIVACY LAWS AND BUSINESS, Cambridge (2017, July 4), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/promoting-privacy-with-innovation-within-the-law/, last accessed 2018/02/18
15. Doneda, D. Da privacidade à proteção de dados pessoais. Renovar, Rio de Janeiro, Brasil (2006).
16. Duhigg, C. How companies know your secrets. The New York Times (2012, February), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp, last accessed 2018/02/20
17. Fisher, D. FTC warns of security and privacy risks in IoT devices. On The Wire (2016, June 3), www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/, last accessed 2018/02/22
18. Fisher, D. The Internet of dumb things. Digital Guardian (2016, October 13). Retrieved from https://digitalguardian.com/blog/internet-dumb-things, last accessed 2018/02/27

19. Ftc Staff Report. Internet of things: privacy & security in a connected world. [S.n.], [s.l.] (2015), www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, last accessed 2017/11/20
20. Global Pulse. Big Data for Development: Challenges and Opportunities. [s.n.], New York (2012), http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-GlobalPulseMay2012.pdf, last accessed 2017/11/15
21. Grassegger, H., & Krogerus, M. The data that turned the world upside down. Motherboard (2017, January 28), https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win, last accessed 2018/02/18
22. Haupt, M. "Data is the New Oil"—A Ludicrous Proposition. Medium (2016), https://medium.com/twenty-one-hundred/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294, last accessed 2017/11/15
23. Kuneva, M. Keynote Speech. Roundtable on Online Data Collection, Targeting and Profiling (2009), http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm, last accessed 2017/11/15
24. Landim, W. Wearables: será que esta moda pega? Tec Mundo (2014, January), www.tecmundo.com.br/tecnologia/49699-wearables-sera-que-esta-moda-pega-.htm, last accessed 2017/11/18
25. Lane, J. et al. (Eds.). Privacy, Big Data and the public good: frameworks for engagement. Cambridge University Press, New York, United States (2014).
26. Leonardi, M. Tutela e Privacidade na Internet. Saraiva, São Paulo, Brasil (2011).
27. Macedo Júnior, R. Privacidade, Mercado e Informação. Justitia, 61, 245-259 (1999).
28. Madden, M. Privacy management on social media sites. Pew Research Center's Internet & American Life Project (2012, February 24), http://www.isaca.org/Groups/Professional-English/privacy-data-protection/GroupDocuments/PIP_Privacy%20mgt%20on%20social%20media%20sites%20Feb%202012.pdf, last accessed 2017/11/19
29. Magrani, Eduardo. The Emergence of the Internet of Things. Internet Policy Review. HIIG, (2017).

30. Magrani, Eduardo. The emergence of the Internet of Anonymous Things (AnIoT). Internet Policy Review – Journal on Internet Regulation (2017, June), https://policyreview.info/articles/news/emergence-internet-anonymous-things-aniot/693, last accessed 2017/12/15
31. Mcdonald, A. M., & Cranor, L. F. The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4(3), 543-568 (2008).
32. Mcnulty, E. Understanding Big Data: the seven V's. Dataconomy (2014, May 22), http://dataconomy.com/2014/05/seven-vs-big-data/, last accessed 2017/11/24
33. Meola, A. How the Internet of things will affect security & privacy. Business Insider (2016, December 19), www.businessinsider.com/internet-of-things-security-privacy-2016-8, last accessed 2017/11/27
34. Molaro, C. Do not ignore structured data in Big Data analytics: the important role of structured data when gleaning information from Big Data. IBM Big Data & Analytics Hub (2013, July 19), www.ibmbigdatahub.com/blog/do-not-ignore-structured-data-big-data-analytics, last accessed 2018/02/01
35. Moraes, M. C. B. Biografias não autorizadas: conflito entre a liberdade de expressão e a privacidade das pessoas humanas? Editorial. Civilistica.com, Rio de Janeiro, 2(2), 1-4 (2013).
36. Mulholland, C. O direito de não saber como decorrência do direito à intimidade. Civilistica.com, Rio de Janeiro, 1(1), 1-11 (2012).
37. Nascimento, R. O que, de fato, é Internet das coisas e que revolução ela pode trazer? Computerworld (2015, March 12).
38. O'Brien, C. Wearables: Samsung chases fitness fans with gear fit 2. The Irish Times (2016, August), www.irishtimes.com/business/technology/wearables-samsung-chases-fitness-fans-with-gear-fit-2-1.2763512, last accessed 2018/02/18
39. Obar, J. A., & Oeldorf-Hirsch, A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. In: The 44th Research Conference on Communication, Information and Internet Policy (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465, last accessed 2017/12/15

40. Oliveira, M. Em marketing, Big Data não é sobre dados, é sobre pessoas! Exame (2016, October), http://exame.abril.com.br/blog/relacionamento-antes-do-marketing/em-marketing-bigdata-nao-e-sobre-dados-e-sobre-pessoas/, last accessed 2017/12/20
41. Palmer, Michael. Data is the new oil. ANA Marketing Maestros (2006, November), http://ana.blogs.com/maestros/2006/11/data_is_the_new.html, last accessed 2017/12/11
42. Plouffe, J. The ghost of IoT yet to come: the Internet of (insecure) things in 2017. Mobile Iron (2016, December 23), www.mobileiron.com/en/smartwork-blog/ghost-iot-yet-come-internet-insecure-things-2017, last accessed 2018/01/18
43. Poikola, A., Kuikkaniemi, K., & Honko, H. MyData - A Nordic Model for human-centered personal data management and processing. Ministry of Transport and Communications ([s.d.]), https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/, last accessed 2018/01/12
44. Post, R. C. Three Concepts of Privacy. Georgetown Law Review, 89, 2087-2098 (2001).
45. Redação. Parlamento Europeu reforça proteção dos dados pessoais dos cidadãos. Parlamento Europeu (2014, March).
46. Redação. Varejista norte-americana descobre até gravidez de clientes com a ajuda de software. Olhar Digital (2012, February), https://olhardigital.com.br/noticia/varejista-norte-americana-descobre-gravidez-de-clientes-com-a-ajuda-de-software/24231, last accessed 2018/01/30
47. Rijmenam, M. Why the 3 V's are not sufficient to describe Big Data. DATAFLOQ (2015, August), https://datafloq.com/read/3vs-sufficient-describe-big-data/166, last accessed 2018/01/18
48. Rodotà, S. A vida na sociedade de vigilância – a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Renovar, Rio de Janeiro, Brasil (2008).
49. Rodrigues, A., & Santos, P. A ciência que faz você comprar mais. Galileu, ([s.d.]), http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-

17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html, last accessed 2018/02/18

50. Roman, R., Zhou, J., & Lopez, J. On the features and challenges of security and privacy in distributed Internet of things. Computer Networks, 57, 2266-2279 (2013).
51. Rose, K., Eldridge, S., & Chapin, L. The Internet of things: an overview. Understanding the issues and challenges of a more connected world. The Internet Society (2015, October), www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf, last accessed 2018/01/19
52. Santos, M. W. O Big Data somos nós: a humanidade de nossos dados. Jota (2017, March 16), https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017, last accessed 2018/01/19.
53. Sarlet, I. W., Marinoni, L. G., & Mitidiero, D. Curso de Direito Constitucional. Editora Revista dos Tribunais, São Paulo, Brasil (2012).
54. Sjöberg, M. et al. Digital Me: Controlling and Making Sense of My Digital Footprint. In: Gamberini, L. et al (Eds.). Symbiotic Interaction: Lecture notes in computer science (pp. 155-156). Springer, Padua, Italy (2016).
55. Sloan, R. H., & Warner, R. (2014). Unauthorized Access: The Crisis in Online Privacy and Security CRC Press, London, England & New York, United States (2014).
56. Venturini, J. et al. Terms of Service and Human Rights: an analysis of online platform contracts. Revan, Rio de Janeiro, Brasil (2016).
57. Warren, S. D., & Brandeis, L. D. The Right to Privacy. Harvard Law Review 4(5), 193-220 (1890).