
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

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

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 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

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.

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 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

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;".

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,

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.

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].

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].

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 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].

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 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).

MODELO INTEGRADO DE ATIVIDADES PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS

JOSÉ MARTINS

HENRIQUE SANTOS

JORGE CUSTÓDIO

&

RUI SILVA [1]

1 jose.carloslm@gmail.com, Academia Militar / CINAMIL, FeelSec Consulting
hsantos@dsi.uminho.pt, Dep. Sistemas de Informação, Universidade do Minho
jorge.filipe.custodio@gmail.com, FeelSec Consulting
& rs.beja@gmail.com, Instituto Politécnico de Beja / UbiNET

RESUMO

Este artigo propõe um modelo que identifica e agrupa em seis dimensões as atividades que contribuem, nas organizações, para a Gestão da Segurança da Informação, a Cibersegurança e a Proteção de Dados Pessoais. O Modelo está orientado para apoiar a atividade profissional dos *Chief Information Security Officer* (CISO), dos Encarregados de Proteção de Dados, dos Consultores e Gestores de Projetos que procuram possuir uma visão holística e integrada destas temáticas. O modelo proposto tem uma abordagem sistémica, na qual se procuram identificar métodos, técnicas e ferramentas de diferentes domínios científicos para a gestão destas temáticas. É suportado numa revisão de literatura, na experiência dos autores resultante da sua atividade académica, auditorias e implementação de Sistemas de Gestão de Segurança da Informação, bem como de projetos de *desenho* e implementação de Sistemas de Informação (SI). É um trabalho de *Design Science* em progresso, através do qual irá ser validado o modelo proposto através da aplicação de um questionário a especialistas *e* da utilização do método de investigação *Action Research*. Como principal resultado obtido deste estudo, salienta-se o modelo de atividades integrado para Gestão de Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais.

Palavras-Chave: Segurança da Informação; Cibersegurança; Proteção de Dados Pessoais; Modelo Integrado de Segurança; Competências de um CISO.

1. INTRODUÇÃO

Na atual Sociedade em Rede, onde as ameaças à informação e aos Sistemas de Informação (SI) são permanentes e evolutivas, é necessário que os atores com responsabilidades nos processos de decisão relativos à Gestão da Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais nas organizações (e.g., CIO, CISO) possuam uma visão de conjunto e integrada. Existe ainda, um conjunto de especialistas que necessitam de um modelo que lhes permita sistematizar e estruturar as atividades e o conhecimento relacionados com as tarefas profissionais que, diariamente, lhe são solicitadas no âmbito destas temáticas.

A multidimensionalidade do problema, bem como a sua complexidade, exige um modelo que reflita uma abordagem multidisciplinar e sistémica. Deste modo, foram consideradas, para o *desenho* do modelo, as seguintes dimensões: (i) *Organização*; (ii) *Adversário*; (iii) *Capacidade de Proteção*; (iv) *Planeamento*; (v) *Gestão Operacional*; (vi) *Formação, Sensibilização e Treino* (Figura 1).

Figura 1: Modelo Integrado de Segurança

Cada uma das dimensões referenciadas na Figura 1 agrega um conjunto de sub-dimensões, que representam atividades profissionais nucleares para a gestão da segurança, que, direta ou indiretamente, contribuem para garantir a confidencialidade, integridade e disponibilidade da informação processada, transmitida e armazenada.

Estas seis dimensões resultam de uma abordagem *bottom-up*, predominantemente interpretativa, com base na análise e síntese documental das referências indicadas para cada uma das sub-dimensões (Tabelas 1 a 6). Esta conceptualização é ainda suportada na experiência dos autores resultante: (i) da sua atividade académica; (ii) da execução de auditorias e implementação de Sistemas de Gestão de Segurança da Informação (e.g., ISO/IEC 27001); (iii) da formulação de projetos de *desenho* e implementação de SI; (iv) bem como na administração de infraestruturas na realização de testes de intrusão.

Possivelmente existem sub-dimensões/atividades não identificadas no modelo proposto, mas acredita-se que todas as referenciadas neste artigo são as mais relevantes, quer no planeamento ou implementação, quer na melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI), que, simultaneamente, se interligue com a Cibersegurança e a Proteção de Dados Pessoais.

Constata-se, através da revisão de literatura, a existência de diversas abordagens relativas à Gestão da Segurança da Informação e à Cibersegurança, sendo comum a todas elas a necessidade de realizar uma identificação e avaliação de riscos dos ativos e dos processos de negócio, seguido do endereçamento dos mesmos através da implementação de controlos de segurança de diferentes classes (e.g., tecnológicos, físicos, administrativos) em função das estratégias para a gestão das ameaças. No entanto, mesmo com níveis de maturidade elevados nos controlos implementados é necessário, ainda, ter planos de contingência (e.g., de *disaster recovery*), pois o risco residual permanecerá e o incidente certamente que ocorrerá, mais cedo ou mais tarde.

Estas abordagens, têm por suporte, na sua maioria, o modelo de gestão conhecido por PDCA *(Plan, Do, Chek e Act)*, o qual procura, em permanência, a melhoria contínua do SGSI. O modelo proposto neste artigo identifica atividades que permitem instanciar estas fases, embora não forneça, ainda, um método que as permita relacionar.

Da análise das abordagens de segurança ao nível organizacional identificam-se como principais dimensões de segurança a: (i) Física e Ambiental; (ii) Humana; (iii) Tecnológica; (iv) Organizacional; em função das quais os principais controlos de segurança podem ser implementados e geridos.

De forma a descrever o modelo proposto o artigo está estruturado em oito seções. Na primeira enquadra-se o problema. Posteriormente, na segunda analisam-se as principais atividades necessárias para conhecer a *Organização*. A terceira seção foca-se nas possíveis ações maliciosas / métodos de ataque do *Adversário* e a quarta nas *Capacidades de Proteção* disponíveis atualmente. Na quinta discutem-se as atividades que contribuem para o *Planeamento*. Seguidamente, na sexta seção descrevem-se as atividades de *Gestão Operacional e* na sétima as centradas na *Formação, Sensibilização e Treino* dos colaboradores da organização. Por fim, na oitava apresentam-se os principais resultados da investigação, as limitações do estudo e alguns dos possíveis os trabalhos futuros a realizar.

2. A ORGANIZAÇÃO

Para realizar a gestão dos controlos de Segurança implementados, ou a aplicar, no âmbito de um SGSI, da cibersegurança e proteção de dados pessoais, é necessário, em primeiro lugar, conhecer em detalhe a Organização. Esta atividade passa, fundamentalmente, por conhecer: (i) o seu ambiente envolvente; (ii) a cultura institucional; (iii) o modelo de gestão; (iv) os processos de negócio; (v) a arquitetura dos Sistemas de Informação; (vi) e, ainda, os dados e a informação (e conhecimento) associados aos processos de negócio (Figura 2).

Figura 2: Conhecer a Organização

O conhecimento do ***Ambiente Envolvente*** permite identificar, de forma macro, algumas das principais ameaças que pendem sobre os ativos da organização. Em relação à ***Cultura Organizacional*** é necessário considera-la na gestão da mudança associada à execução das atividades de segurança, tendo em consideração os comportamentos predominantes dos funcionários da Organização e dos colaboradores externos.

Por outro lado, conhecer o ***Modelo de Gestão*** implementado na organização (e.g., Sistema de Gestão Integrado baseado na ISO/IEC 9001), permitirá, mais facilmente, alinhar os controlos de segurança a implementar com os objetivos estratégicos e operacionais do negócio. Simultaneamente, a análise dos ***Processos de Negócio*** da cadeia de valor, permite identificar a informação nuclear para o negócio e os ativos críticos a proteger.

É, ainda, necessário conhecer a ***Arquitetura dos SI*** da Organização, onde se inclui a infraestrutura tecnológica de suporte (i.e., a sua rede de computadores), que é um elemento essencial no processo de conhecer as respetivas vulnerabilidades. E, por fim, é determinante conhecer os ***Dados / Informação*** que integram os processos de negócio, considerando-se fundamental identificar o seu ciclo de vida, o seu valor e a sua classificação de segurança.

Nas sub-dimensões que contribuem para a análise da Organização podem-se utilizar Métodos, Técnicas e Ferramentas (MTF) (Tabela 1) com origem em outras áreas do conhecimento (e.g., Gestão, Sistemas de Informação, Sociologia, Psicologia), de validade científica ou profissional comprovada, que podem ser úteis ao especialista no *desenho* e na gestão de um SGSI, o que reforça a necessidade dos especialistas nestas temáticas terem uma visão holística e multidisciplinar.

Tabela 1: Conhecer a Organização

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Ambiente Envolvente	Técnicas de Gestão (e.g., PESTAL, PORTER, SWOT)	(Teixeira, 2005)
Cultura Organizacional	Tipologia de Culturas (e.g., Comunidade)	(Robbins, 2002)
Modelo de Gestão	Sistema de Gestão integrado	(Teixeira, 2005); (ISO/IEC 9001, 2015)
Processos de Negócio	Modelação de Processos (e.g., BPMN)	(Weske, 2007)
Arquitetura de SI	Framework de Zackman; TOGAF	(Greefhorst, Danny and Proper, 2011); (Laudon e Laudon, 2006); (Turban, Rainer e Potter, 2003)
Dados, Informação e Conhecimento	Ciclo de Vida da Informação; Valor Informação; Classificação da Informação	(Gleick, 2006); (Nonaka e Takeuchi, 1995); (Santos e Isabel, 2006)

Nos MTF referenciados na Tabela 1 e posteriores (Tabelas 2 a 6), a preocupação principal dos autores é deixar ao leitor *referências* sobre estas temáticas. Conhecer a Organização em detalhe permite, certamente, aumentar a eficiência e eficácia do SGSI implementado, pois exige-se uma *Arquitetura de Segurança* integrada com o seu modelo de negócio.

3.O ADVERSÁRIO

Após a análise da Organização é necessário conhecer o Adversário (Figura 3). Esta atividade passa fundamentalmente por conhecer: (i) o campo de ação onde este atuará; (ii) os principais atores que o podem tipificar; (iii) os seus possíveis vetores e métodos de ataque; (iv) as vulnerabilidades que este procurará explorar; (v) as técnicas de simulação de métodos de ataque que permitem treinar as modalidades de ação de um adversário, de modo a selecionar a forma mais eficiente e eficaz de aplicação dos controlos para a proteção da Organização; (vi) a doutrina associada às *Computer Network Operations, especialmente a militar*, pois estas representam, em termos de intenção e capacidade de um hipotético adversário, o pior cenário defensivo para as Organizações, num possível ambiente conflitual.

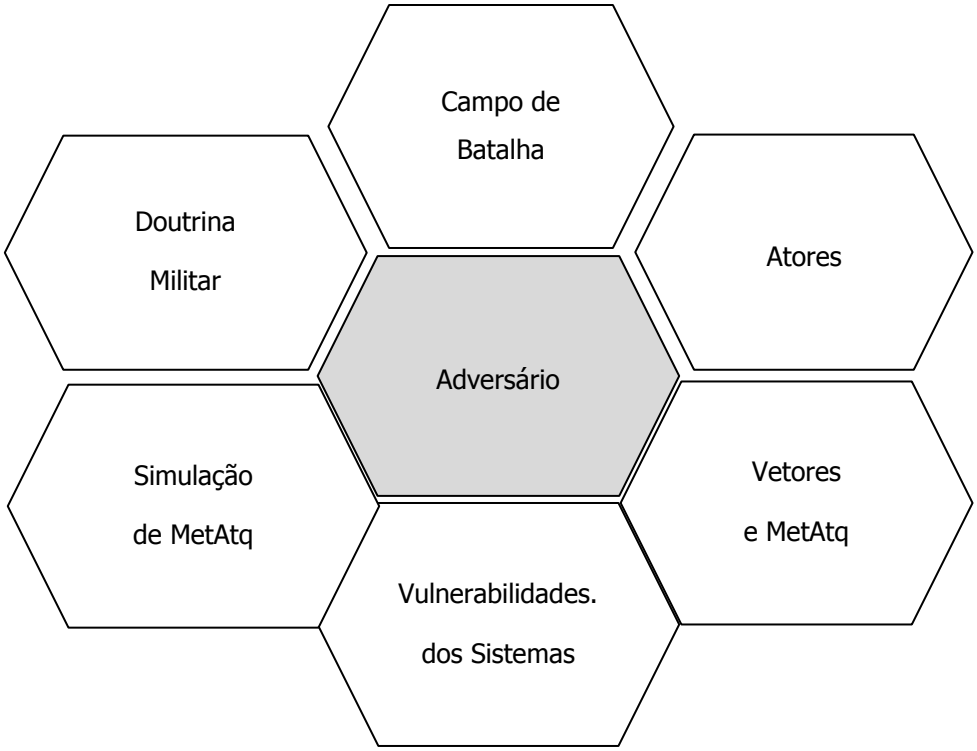

Figura 3: Conhecer o Adversário

Para poder endereçar os riscos de Segurança da Informação e Cibersegurança, ou numa perspetiva bélica, ter capacidade de fazer face aos métodos de ataque de um adversário é necessário conhecer em primeiro lugar o ***Campo de Batalha***, i.e., o ambiente onde este atua. Consequentemente, é essencial ter conhecimento sobre o funcionamento e estrutura das redes de computadores, da Internet, componentes aplicacionais existentes e, ainda, das linguagens de programação e suas vulnerabilidades.

É, também, importante ter a perceção de quais poderão ser os principais ***Atores*** a interagir de forma maliciosa com a Organização. Subsequentemente, é necessário conhecer os seus níveis de atuação (chamados eixos de aproximação do Inimigo, em doutrina militar) e os possíveis ***Métodos de Ataque*** (ações e ferramentas utilizadas), através dos quais procurarão explorar as vulnerabilidades identificadas relativamente aos ativos da Organização.

Estas ações numa Organização podem ser executadas segundo três níveis de ataque principais: o físico, o humano e o da infraestrutura tecnológica, que são suscetíveis de poder comprometer as propriedades fundamentais de segurança da informação, i.e., a confidencialidade, integridade e disponibilidade.

A execução de um método de ataque, i.e., de uma ação ou conjunto de ações maliciosas por parte de um adversário, visa explorar uma ou mais vulnerabilidades (debilidades dos Sistemas, resultantes do seu desenho, parametrização, administração ou utilização) de um determinado Sistema. Estes métodos de ataque podem e devem ser simulados pelas Organizações, em ***ambientes controlados***, de forma a testar soluções de segurança, sensibilizar e treinar os colaboradores a responder a incidentes, bem como validar os seus planos de contingência (e.g., *Disaster Recovery*).

Uma análise mais detalhada em termos da possível atuação de um adversário, i.e., das suas possíveis modalidades de ação, pode ser complementada através do estudo da ***Doutrina Militar*** de Operações de Informação, onde as *Computer Network Operations* são uma das capacidades fundamentais ou de *Frameworks de Testes de Intrusão.*

Se, numa primeira iteração, os requisitos de segurança da Organização associados às propriedades de Segurança da Informação e os ativos críticos que fazem parte dos processos de negócio são essenciais para as organizações orientarem o planeamento, uma segunda iteração é fundamental a identificação dos vetores e métodos de ataque, procurando, se possível, identificar as modalidades de atuação do adversário mais prováveis (com maior probabilidade de ocorrer) e as de maior impacto.

Ao nível físico, podem considerar-se, a título exemplificativo, ações maliciosas sobre as instalações físicas, os equipamentos (e.g., o *hardware),* os sistemas de suporte (e.g., sistema de energia elétrica), os documentos em suporte físico (e.g., sabotagem, roubo) e as próprias pessoas (e.g., especialistas com funções essenciais na organização).

É, ainda, fundamental salientar a importância da prevenção de catástrofes naturais (e.g. pandemias, tremores-de-terra) ou desastres (e.g. incêndios, inundações), de forma a garantir, também, a Segurança da Informação (e.g., disponibilidade). Estes incidentes, a ocorrerem, tem consequências sobre determinados componentes dos SI, nas instalações ou nos respetivos processos de negócio (inclui os recursos humanos).

Ao nível da infraestrutura tecnológica, as ações maliciosas podem ser executadas sobre aplicações diversas (e.g., Sistemas Operativos, Bases de Dados). Estas ações possibilitam, também, alterar o funcionamento da sua rede de computadores, através de acesso interno, ou externo (e.g., através da Internet), e explorar vulnerabilidades dos serviços implementados.

Finalmente, ao nível humano, deve dar-se especial atenção às ações que possibilitem: (i) manipular os colaboradores (internos e externos) da Organização (e.g., ataques de *phishing*); (ii) criar falsas perceções nos decisores para uma determinada situação; (iii) e ainda alterar os processos de decisão implementados.

Existem, também, nesta dimensão alguns MTF que podem ser utilizadas para obter um conhecimento mais pormenorizado do adversário e que estão referenciadas na Tabela 2.

Tabela 2: Conhecer o Adversário

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Campo de Batalha	Redes de Computadores Públicas e Privadas (protocolo TCP-IP, ativos de rede).	(Kurose e Ross, 2010); (Knapp e Langill, 2015); (Correia e Sousa, 2010)
Atores	Taxonomias de Atores (e.g., Intel TARA)	(Carr, 2012); (Andress e Winterfeld, 2011); (Waltz, 1998)
Vetores e Métodos de Ataque	Frameworks de MetAtq (e.g., CAPEC, OWASP)	(Pfleeger e Pfleeger, 2012); (Gregg, 2006); (Wantson, Mason e Ackroyd, 2014)

Vulnerabilidades dos Sistemas	Taxonomias de Vulnerabilidades (e.g., CVS, NVD)	https://nvd.nist.gov; http://www.cve.mitre.org (consultados em 27 de Dezembro de 2017)
Simulação de Métodos de Ataque	Frameworks de Testes de Intrusão, Técnicas (e,g., árvores de ataque, cenarização), Ferramentas (e.g., KALI)	(NIST 800-115, 2008); (Shostack, 2014); Martins, Santos, Nunes and Silva (2012b)
Doutrina Militar	Operações de Informação e *Computer Network Operations*	(FM 3-13, 2003); (JP 3-13, 2012); (JP 3-12, 2013); (FM 3-38, 2014)

Após abordar a perspetiva do adversário, identificam-se na próxima seção as principais capacidades de proteção atualmente disponíveis, que permitem à Organização garantir a Segurança da Informação, Cibersegurança e a Proteção de Dados.

4.AS CAPACIDADES DE PROTEÇÃO

Após conhecer a Organização e o Adversário, é necessário ter uma visão atual das *Capacidades de Proteção* disponíveis, i.e., o "*Estado-da-Arte"* (Figura 4) e que passa fundamentalmente por conhecer: (i) os princípios e postulados da segurança; (ii) as principais disciplinas académicas de referência que suportam estas temáticas; (iii) as tecnologias de segurança existentes; (iv) as normas internacionais ou nacionais e as certificações reconhecidas pela Industria; (v) a legislação e a regulamentação da área de negócio da Organização com obrigatoriedade jurídica de cumprimento; (vi) e ainda a

interligação entre capacidades Defensivas vs. Ofensivas, ou seja, que controlos de segurança aplicar para métodos de ataque específicos.

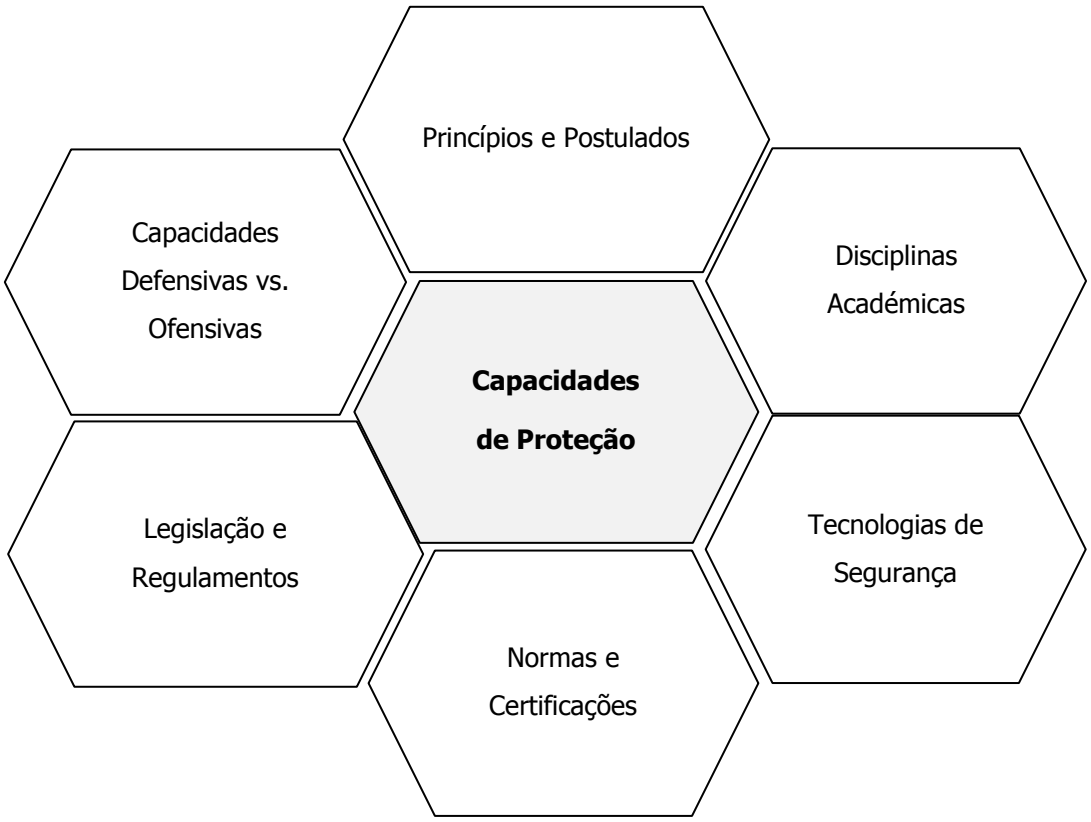

Figura 4: Conhecer as Capacidades de Proteção

Em primeiro lugar deve-se orientar a Segurança da Informação e a Cibersegurança por um conjunto de ***Princípios e Postulados*** que são suportados na experiência dos especialistas e unanimemente aceites, dos quais se salientam: (i) *"a defesa em profundidade" (i.e., múltiplas camadas de proteção); (ii) "a necessidade de conhecer"; (iii) e "o mínimo privilégio".*

É, também, obrigatório considerar-se o conhecimento das ***Disciplinas Académicas*** de referência que suportam estas temáticas, como sejam, e principalmente: (i) a criptografia; (ii) a segurança de redes de computadores; (iii) a segurança da Internet; (iv) e a segurança no *software*.

Por outro lado, é necessário considerar a utilização de boas práticas ou recomendações de segurança já aceites pelos especialistas e que se encontram muitas delas já refletidas em ***Normas*** Internacionais (e.g., ISO / IEC 27001, ISO / IEC 27032), Nacionais (e.g., NIST 800-53 / EUA), ou em ***Certificações*** (e.g., CISSP). Deve, ainda, garantir-se a utilização de tecnologias que atualmente são *Commodities de Segurança* (e.g., *firewall*, antivírus).

É, ainda, fundamental considerar os ***Regulamentos*** do setor de negócio da Organização, bem com a ***Legislação*** em vigor no País em que exerce atividade. Atualmente um dos aspetos mais relevantes e obrigatórios para as Organizações com sede na União Europeia é o cumprimento do Regulamento Geral de Proteção de Dados (EU 2016 / 679), sendo critico, em termos de segurança, o cumprimento do Art.º 32.º (Segurança do Tratamento).

Um aspeto nuclear nesta dimensão é a capacidade de ***Interligar as Modalidades de Ação*** do adversário, ou seja, os seus métodos de ataque, com controlos de Segurança da Informação ou Cibersegurança, procurando, continuamente, melhorar a sua eficiência e eficácia, através da avaliação do nível de maturidade destes para endereçar os riscos identificados pela Organização. Existem alguns MTF que estão disponíveis para apoiar o *desenho* e implementação de um SGSI e que são referenciadas na Tabela 3.

Tabela 3: Conhecer as Capacidades de Proteção

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Princípios e Postulados	Defesa em Profundidade, Necessidade de Conhecer, Mínimo Privilégio	(NIST 800-27, 2004); (Dhillon, 2007);

Tabela 3: Conhecer as Capacidades de Proteção		
Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
		(Pfleeger e Pfleeger, 2007); (Smith, 2013); (Whitman e Mattord, 2012)
Disciplinas Académicas	Criptografia, Segurança de SI; Segurança de Redes, Segurança da Internet, Segurança no Software	(Stallings, 2011); (Dhillon, 2007); (Zúquete, 2007); (Touhill e Touhill, 2014); (Correia e Sousa, 2010)
Tecnologias de Segurança	Firewall, Antivírus, SIEM, Gestão de Identidades e Acessos	(Venter e Eloff, 2003)
Normas e Certificações	ISO / IEC 27001, NIST 800 – 53, Frameworks de Cibersegurança, CISSP	(ISO 27001, 2013); (NIST 800 – 53, 2013); (ISO 27032, 2012); (CISSP_CKB, 2013); SANS (2013); (Martins and Santos, 2010)
Legislação e Regulamentos	Lei da Cibercriminalidade, Regulamente de Proteção de Dados, Legislação de Segurança Nacional	(Fazendeiro, 2017)

Tabela 3: Conhecer as Capacidades de Proteção		
Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Capacidades Defensivas vs. Ofensivas	Modelos de Apoio à Decisão (e.g., Teoria dos Jogos), Cenarização (e.g., Análise Morfológica Geral)	(Martins, 2015); (Ritchey, 2010)

A revisão de literatura realizada, permitiu identificar métodos e normas orientados para: (i) a gestão do risco da Segurança da Informação (e.g. OCTAVE, ISO/IEC 27005); (ii) normas de certificação e boas práticas de gestão de Segurança da Informação e de SI (e.g. ISO/IEC 27001, ISO/IEC 27002, NIST 800-53); (iii) e normas e boas práticas de segurança com foco tecnológico (e.g. ISO/IEC 13335-4, NIST 800-54). Existem, também, normas orientadas à certificação do produto ou Sistema (e.g. ISO/IEC 15408) e normas para avaliar a maturidade dos processos de segurança de uma organização (e.g. ISO/IEC 21827).

Por fim, identificam-se, também, normas da Indústria que embora mais orientadas aos processos de negócio (e.g. CobiT5) e à gestão das TI (e.g. ITIL V3, ISO/IEC 20000), que refletem uma preocupação com a Segurança da Informação. Salienta-se, ainda, a possível aplicação dos controlos referenciados em algumas das principais abordagens de Cibersegurança, como sejam: (i) as recomendações da ISO / IEC 27032; (ii) a *framework* de Cibersegurança do NIST; (iii) as boas práticas da ENISA; (iv) ou os 20 controlos de Ciberdefesa indicados pela SANS, muitos dos quais também sugeridos pelas abordagens de Segurança da Informação atrás referenciadas.

Nas abordagens de Segurança da Informação e Cibersegurança em apreço, é comummente aceite que as propriedades fundamentais da segurança da informação são a confidencialidade, a integridade e a disponibilidade, sendo necessário garantir que tais propriedades não são afetadas: (i) por ações maliciosas ou negligentes realizadas por elementos externos ou internos à Organização; (ii) pela ocorrência de catástrofes

naturais ou desastres internos; (iii) ou pela execução de eventos não previstos ocorridos nos ativos tecnológicos implementados (e.g., falhas).

Em termos da proteção de dados, o regulamento no Art.º 32º - Segurança do Tratamento, refere a importância de aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco e a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. Certamente que as abordagens identificadas anteriormente terão os controlos necessários e, eventualmente, suficientes para garantir esta proteção.

Esta dimensão permite conhecer algumas das principais abordagens para a gestão da Segurança da Informação e Cibersegurança *(Estado-da-Arte)*, as tecnologias de segurança disponíveis e ainda as obrigações legais e regulamentares das organizações.

5.O PLANEAMENTO

Após conhecer a Organização, as capacidades do Adversário e as Capacidades de Proteção existentes, está-se na posse dos elementos mais relevantes para iniciar o Planeamento de um SGSI (Figura 5), o qual pode ser definido como o processo de determinar, antecipadamente (inclui previsão), o que deve ser feito, por quem, quando e como fazê-lo. Nesta dimensão é fundamental saber: (i) analisar sistemas complexos; (ii) especificar requisitos e modelar processos; (iii) identificar, avaliar e estimar riscos; (iv) efetuar o *design* de políticas de segurança; (v) e de planos de contingência; (vi) e, ainda, gerir projetos (projetar o planeamento na implementação, através de um método).

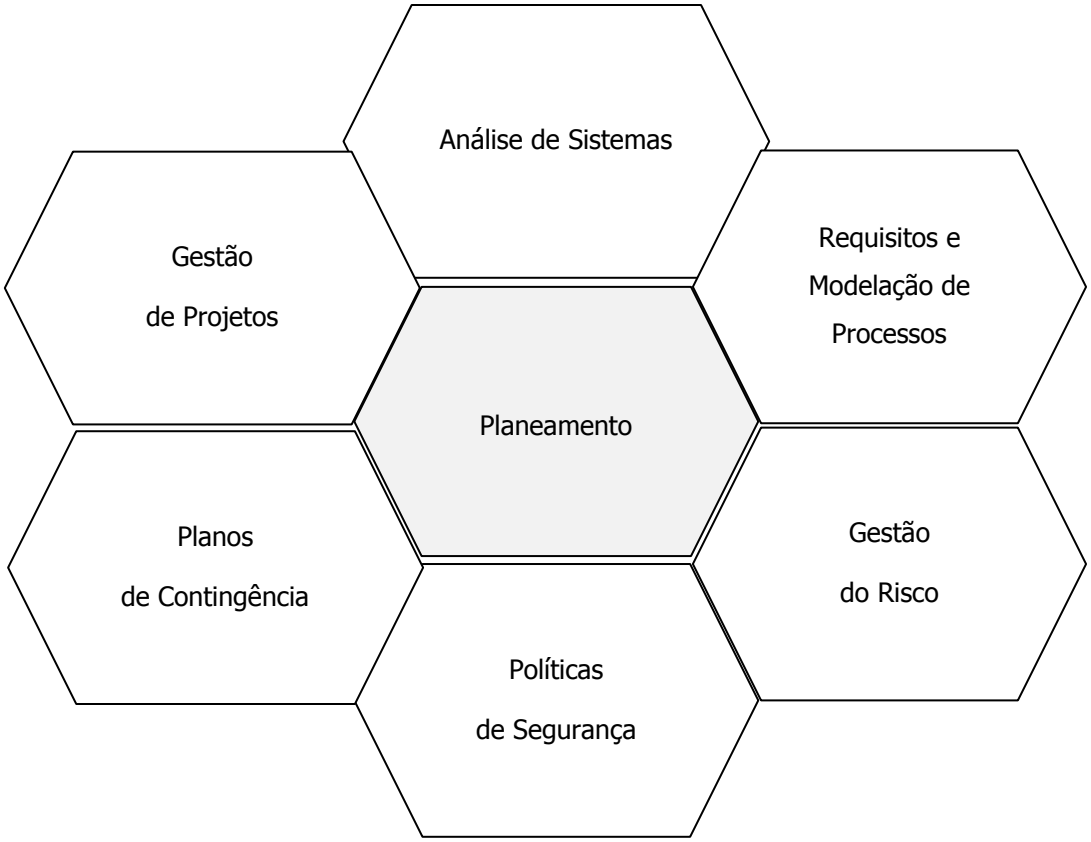

Figura 5: Planeamento da Segurança

Uma primeira atividade fundamental, é a capacidade de efetuar a ***Análise de Sistemas*** complexos, i.e., com múltiplas variáveis, e de definir com rigor os ***Requisitos*** que um SGSI deve ter, bem como efetuar o *desenho* do seu processo de gestão operacional e a interligação com todos os outros processos de negócio da organização.

Outra atividade central no planeamento é a ***Identificação e Avaliação de Riscos*** dos ativos críticos para o negócio, de modo a, posteriormente, se implementar o plano de tratamento.

Esta atividade deve ser o centro de gravidade do planeamento, pois permite interligar as principais variáveis do problema (ameaças, ativos, vulnerabilidades, controlos).

É nuclear que o SGSI seja suportado por um conjunto de ***Politicas de Segurança da Informação*** (e.g., Politica de Segurança da Informação) e ***Planos de Contingências*** (e.g., *Disaster Recovery*). Deve, ainda, garantir-se no planeamento que a implementação dos controlos do SGSI seja realizada de acordo com as melhores

práticas de ***Gestão de Projetos***, testando, se possível, a sua implementação em ambiente de desenvolvimento e qualidade, antes da sua implementação em ambiente de produção.

Um aspeto a ter em conta na criação das políticas / planos e na gestão de projetos é a existência de uma linguagem comum (e.g., taxonomia) que permita que diferentes atores tenham o mesmo entendimento do problema.

Para efetuar o planeamento existe um conjunto de MTF (Tabela 4) que poderão apoiar, e cuja indicação neste artigo resulta da aplicação das mesmas pelos autores em diversos projetos empresariais, que permitiram suportar a fase de análise e desenho de processos de Segurança da Informação ou Cibersegurança.

Tabela 4: Métodos, Técnicas e Ferramentas de Planeamento

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Análise de Sistemas	Questionários, *Focus Group*, Entrevistas, Diagramas de Causa-Efeito	(Eaton, Redmayne and Thordsen, 2007); (Liamputtong, 2011); (Remenyi, 2012)
Requisitos e Modelação de Processos	*UML - Use Cases*, BPMN	(Silva e Videira, 2005); (Wiegers e Beatty, 2013)
Gestão do Risco	Técnicas qualitativas ou quantitativas	(ISO 31000, 2012); (ISO 31010, 2016); (ISO 27005, 2011)

Políticas de Segurança	Politica de Segurança da Informação, Políticas Técnicas, Instruções Operacionais	(Sá Soares, 2004); (CISSP_CBK, 2013); (NIST 800-18, 2006)
Planos de Contingência	Incidentes e Problemas, Disaster Recovery, Continuidade de Negócio, Gestão de Crises	(Whitman, Mattord e Green, 2014); (NIST 800-34, 2010); (ISO 22301, 2012)
Gestão de Projetos	PMBOK, APMI, SCRUM	(PMBOK, 2013); (Hermarij, 2013); (Sutherland, 2014)

Após planear, é necessário implementar o SGSI ("*To Be*"), o qual deve ser realizado de forma iterativa e em que, na maioria das vezes, se utilizam controlos de segurança que já estão implementados na Organização, os quais são identificados e avaliados nas atividades de análise da Organização ("*As Is*"). Um aspeto fundamental é, ainda, considerar, desde o início de um projeto para desenvolvimento de um produto, processo, ou serviço, a Segurança da Informação. Após a implementação de um SGSI é fundamental a sua Gestão Operacional, dimensão esta que será abordada na próxima seção.

6. A GESTÃO OPERACIONAL

As tarefas principais da Gestão Operacional são: Planear (atividade descrita anteriormente), Organizar, Dirigir e Controlar todos os esforços a realizar em todas as áreas / processos de negócio e a todos os níveis da Organização (estratégico, tático e operacional), a fim de garantir os seus requisitos de Segurança. Nesta dimensão identificam-se como principais sub-dimensões: (i) a liderança digital; (ii) a monitorização e as auditorias; (iii) a gestão das Tecnologias de Informação; (iv) a gestão da *framework* de controlos de segurança implementados; (v) a resposta a incidentes e recuperação de desastres; (vi) e a continuidade de negócio e gestão de crises (Figura 6).

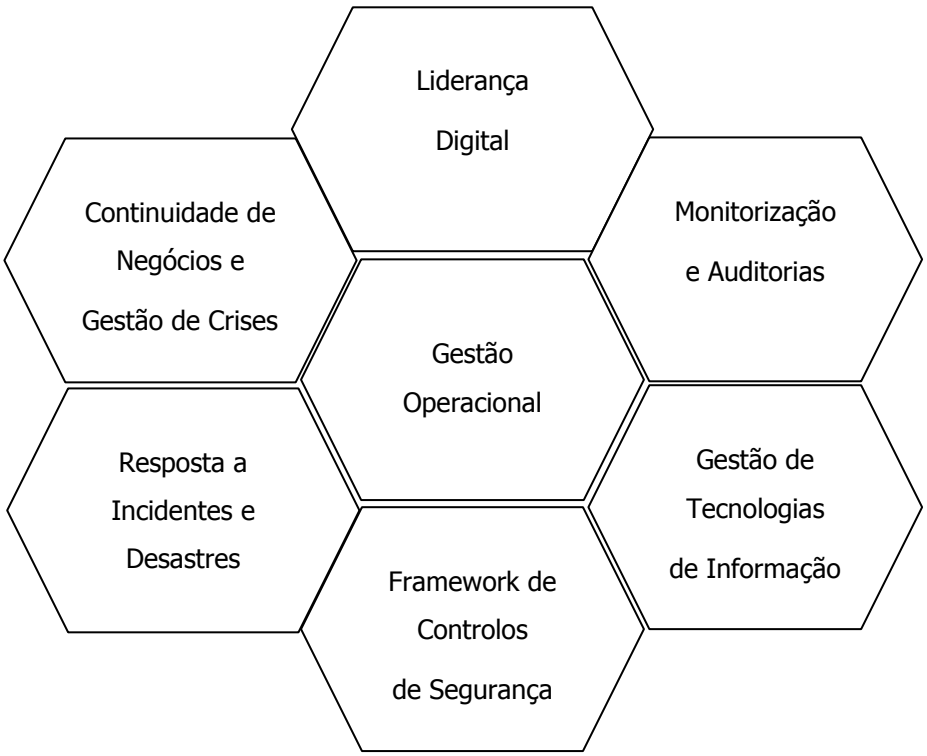

Figura 6: A Gestão Operacional da Segurança

Um dos aspetos fundamentais é a ***Liderança Digital***, que passa fundamentalmente pela gestão dos elementos que gerem a segurança ("Quem Controla o Polícia?"). É necessário também que os decisores considerem nas suas atividades de gestão novas formas de liderar em virtude das suas equipas de TI / Segurança serem na maioria das vezes constituídas por equipas de *Outsourcing*, a trabalhar remotamente através de ambientes colaborativos (equipas virtuais), com limitadas relações pessoais entre os

elementos da equipa, os quais na maioria das vezes tem diferentes nacionalidades, com os constrangimentos que daí resultam.

Outro aspeto essencial é a ***Monitorização e Auditoria*** das ações realizadas sobre os dados / informação armazenada, transmitida ou processada na organização, especialmente a de valor mais elevado (e.g., dados pessoais). Uma possível solução pode passar por possuir: (i) um *Security Information and Event Management,* que centralize e correlacione todos os eventos de segurança da Organização; (ii) e um sistema de gestão de identidades e acessos, que garanta às Organizações, identidades digitais únicas associadas aos colaboradores, em todos os Sistemas, e com perfis de acesso bem definidos.

É, também, importante uma eficiente ***Gestão das Tecnologias de Informação*** da Organização, com especialmente preocupação para a sua disponibilidade e capacidade de suportar os seus processos de negócio. A correta aplicação de boas práticas de gestão das TI permite endereçar muitos dos riscos de Segurança da informação e Cibersegurança.

A componente operacional, ou seja, as operações do dia-a-dia, passa pela gestão de uma ***Framework de Controlos de Segurança*** implementados, cuja estrutura se sugere estar orientada, fundamentalmente, pelas dimensões: (i) Organizacional; (ii) Física e Ambiental; (iii) Humana; (iv) e Tecnológica; que devem proteger dos principais níveis de atuação de um adversário e dos seus métodos de ataque. Nesta *framework* deve-se procurar uma integração de controlos que garanta o propósito de prevenir, detetar, deter, desviar, recuperar e reagir, face aos riscos identificados na Organização, e, simultaneamente, permita a defesa em profundidade e o apoio mutuo entre controlos, através da interligação entre os controlos tecnológicos, os procedimentos / processos e as boas práticas dos utilizadores, em múltiplas camadas de proteção.

A gestão operacional passa por, eventualmente, implementar um *Security Operations Center (SOC)*, com a capacidade mínima para auditar e monitorizar os controlos de Cibersegurança implementados, alguns dos quais associados, também, à Segurança da Informação e certamente à proteção de dados pessoais.

Por outro lado, é importante perceber e aceitar que o incidente vai ocorrer, consequentemente, há necessidade de desenvolver a capacidade de ***Resposta a Incidentes e Recuperação de Desastres***, no mínimo, com planos de contingência operacionais e treinados para a gestão de incidentes e a recuperação de desastres de TI. Será, possivelmente, necessária na execução de algumas ações, a colaboração (e partilha de informação) de entidades externas à Organização (e.g., ISP, Centro de Cibersegurança Nacional, Policia de Investigação Criminal).

É claro que a Organização, numa abordagem holística deve considerar todos os aspetos de segurança no seu plano de ***Continuidade de Negócio***, garantindo que tem capacidade para continuar a entregar produtos ou serviços aos clientes nos níveis acordados e aceitáveis após um incidente.

Tabela 5: Gestão Operacional

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Liderança Digital	Equipas Virtuais	(Ford, Piccolo e Ford, 2017); (Chang, Hung, Hsieh, 2014)
Monitorização e Auditorias	Ferramentas *Open Source* (e.g., GLPI, Nagios); SIEM	(Liska, 2015); (Jacobs e Rudis, 2014); (ISO 19011, 2012)
Gestão de TI	ISO 20000-1, ITIL	(Turban, Rainer e Potter, 2003); (ISO 20001, 2015); (ITIL 3, 2007)
Framework de Controlos de Segurança	Dimensões, Categorias e Controlos; Funcionalidades de um CSIRT	Martins, Santos, Nunes e Silva (2012a);

		Martins, Santos, Rosinha and Valente (2013); (Martins, 2015); (SANS, 2013)
Resposta a Incidentes e Recuperação de Desastre	Processo e Ferramenta de Gestão de Incidentes; Plano de *Disaster Recovery*	(Whitman, Mattord e Green, 2014); (NIST 800-34, 2010); (NIST 800-61, 2012); (ISO 27035, 2011)
Continuidade de Negócios e Gestão de Crises	Plano de Continuidade de Negócio	(Whitman, Mattord e Green, 2014); (ISO 22301, 2012); (BCI, 2013)

Nas dimensões anteriormente descritas existe uma variável cuja *"Parametrização e Controlo"* é quase impossível numa arquitetura de Segurança da Informação e Cibersegurança e que é o "Elemento Humano". A sua manipulação, através de ataques de Engenharia Social, pode pôr em causa todo o processo de segurança ou a tecnologia implementada na Organização, consequentemente, este elemento necessita de formação, sensibilização e treino ajustado a uma realidade complexa e em permanente mudança.

7.A FORMAÇÃO, SENSIBILIZAÇÃO E TREINO

Tal como afirma Peltier, um programa eficaz de Segurança da Informação não pode ser implementado sem promover um programa de treino e consciencialização dos colaboradores, o qual deve endereçar políticas, procedimentos e ferramentas (2005).

Nesta dimensão é fundamental: (i) utilizar técnicas corretas de ensino na transmissão de conhecimento, através de ações de formação, sensibilização e treino, presenciais ou online; (ii) analisar as competências necessárias dos colaboradores nos diferentes níveis da Organização; (iii) desenvolver conteúdos pedagógicos apelativos; (iv) utilizar plataformas de *E / B-learning* para disponibilizar os conteúdos; (v) realizar exercícios coletivos e treino individual; (vi) e por fim, garantir uma gestão de conhecimento focada na gestão das lições apreendidas com incidentes de segurança (Figura 7).

Um aspeto nuclear, é aplicar na formação, sensibilização e treino dos colaboradores, as mais recentes ***Técnicas de Ensino*** (e.g., jogos, ambientes de simulação) ajustadas às audiências e em função das suas necessidades (competências a obter – "*To Be*"). Pressupõe-se, consequentemente, uma prévia identificação das ***Competências dos Colaboradores*** nas temáticas de Segurança da Informação e Cibersegurança ("*As Is*"), bem como a integração destas nas descrições de funções do colaborador e no plano de formação anual da Organização.

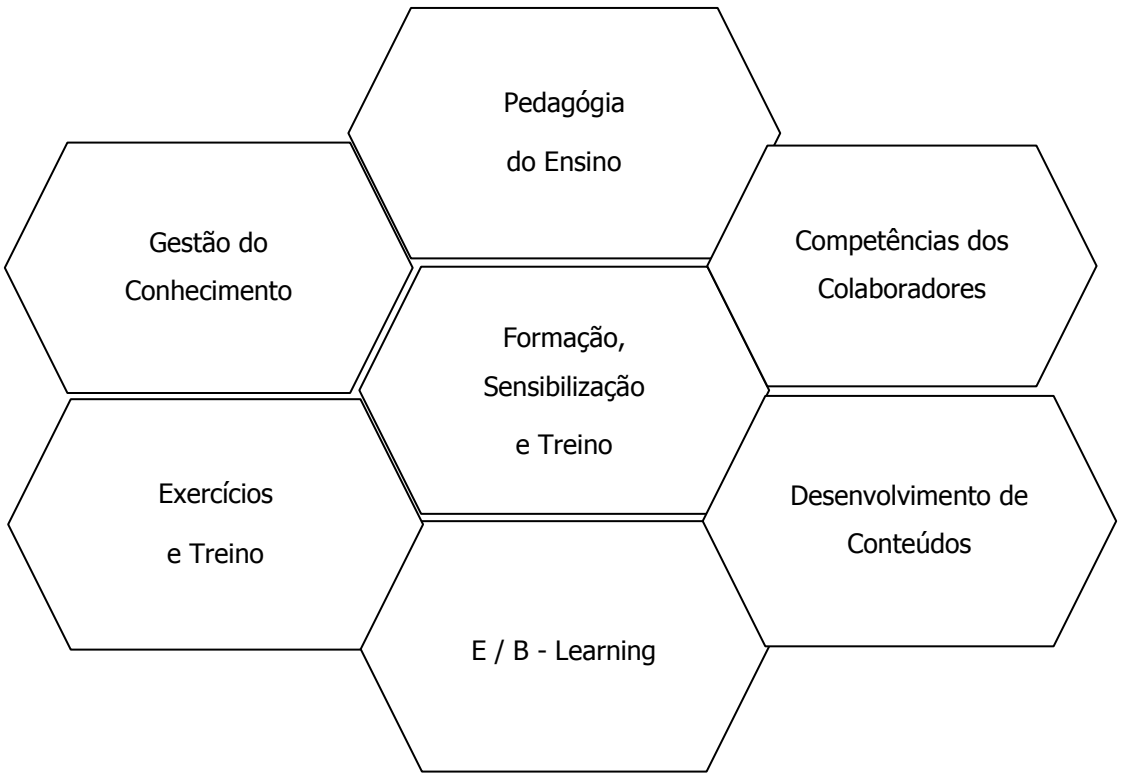

Figura 7: Formação, Sensibilização e Treino

É necessário, também, ***Desenvolver Conteúdos*** para as ações de formação e sensibilização (e.g., jogos), que permitam maior realismo, intervenção dos colaboradores da Organização e que facilitem a "passagem da mensagem", disponibilizando os conteúdos, sempre que possível, através de ***Plataformas de E-learning*** (e.g., Moodle), pelas vantagens que daí resultam.

Algumas das possíveis abordagens passam pela realização de ***Exercícios*** e ***Treino*** dos colaboradores (e.g., reagir a um ataque de *phishing*), pela realização de laboratórios em ambientes de simulação (e.g., *Cross Site Scripting*) ou a participação em exercícios coletivos (e.g., gestão de crises, recolha de informação de fontes abertas - OSINT).

Outro aspeto nuclear é a partilha de experiências, de lições aprendidas entre os colaboradores da Organização. Uma das formas, entre outras, para realizar esta partilha é possuir um processo automatizado para gestão de incidentes (e de problemas), que possibilite disponibilizar *Casos de Estudo* aos que necessitam de os conhecer em função das suas atividades e cujo objetivo principal é evitar a repetição de erros. Garante-se deste modo a ***Gestão de Conhecimento*** na área da Segurança da Informação

Nesta dimensão, existe, também, um conjunto de MTF (Tabela 6), cuja indicação neste artigo resulta da sua aplicação pelos autores em diversas atividades de ensino, de treino militar e ainda em formação certificada.

Tabela 6: Formação, Sensibilização e Treino

Sub-dimensões	**Métodos, Técnicas e Ferramentas (e.g.,)**	**Referências Bibliográficas**
Pedagogia do Ensino	Técnicas de Ensino (e.g., Casos de Estudo)	(Sternberg, Sternberg e Mio, 2012); (Jensen, 2009); (MTP, 2003)
Análise de Competências	Manual de Funções da Organização;	(NIST 800-118, 2017); (NIST 800-16, 2014);

	Plano Anual de Formação	(Peltier, 2005); (Siponen, 2001); (Mann, 2008); (Hadnagy, 2011)
Desenvolvimento de Conteúdos	Jogos de Guerra	(Creveld, 2013); (Dunnigan, 2000); (Michael e Chen, 2005)
Plataformas de E - Learning	Ensino online	(PROLEARN, 2004); (Nash, Susan and Moore, 2014)
Exercícios e Treino	Laboratórios de Simulação, Exercícios (e.g., Gestão de Crises)	(ENISA_ Training, 2014); (NIST 800-50, 2003); (Martins et al., 2016)
Gestão do Conhecimento	Modelos de Gestão do Conhecimento	(Nonaka e Takeuchi, 1995); (PDE_0-32-00, 2012)

Embora todas as Dimensões / Sub-dimensões referenciadas anteriormente sejam fundamentais para o desenho e a implementação de uma eficaz Arquitetura de Segurança da Informação e Cibersegurança, é necessário que esta integre a formação, sensibilização e o treino nestes domínios de todos os colaboradores da Organização.

8.CONSIDERAÇÕES FINAIS

Este artigo propõe um modelo que identifica e interliga algumas das mais importantes, senão a maioria das atividades necessárias para a implementação de um Sistema de Gestão de Segurança da Informação, que simultaneamente considera a Cibersegurança e a Proteção de Dados Pessoais. Modelo este, orientado para a atividade profissional dos CISO, dos Encarregados de Proteção de Dados, dos Consultores e Gestores de Projetos que procuram possuir uma visão holística destas temáticas. O modelo proposto é suportado numa revisão de literatura, na experiência dos autores obtida durante a sua atividade académica, em auditorias e implementação de Sistemas de Gestão de Segurança da Informação e em projetos de *desenho* e implementação de Sistemas de Informação.

Como principais resultados obtidos deste estudo, salientam-se: (i) o modelo para a gestão de Segurança da Informação, Cibersegurança e Proteção de Dados; (ii) e a identificação e sugestão de um possível conjunto de competências profissionais, necessárias para a atividade profissional dos responsáveis pela Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais.

Conclui-se ainda que a gestão da Segurança da Informação, a Cibersegurança e a Proteção de Dados Pessoais nas organizações possuem um conjunto de atividades comuns, que, direta ou indiretamente, contribuem para garantir as propriedades fundamentais de Segurança da Informação.

A principal limitação do modelo proposto passa por apenas descrever, sumariamente, as dimensões / Sub-dimensões, os métodos e as técnicas, e não identificar as interligações entre as Sub-dimensões deste. No entanto, isso deve-se ao facto de se tratar de um trabalho em progresso, onde futuramente *se* procurará que o modelo proposto seja validado através da aplicação de um *questionário* a especialistas nestas temáticas e do método de investigação *Action Research* aplicado a projetos de implementação de SGSI, Cibersegurança ou Proteção de Dados Pessoais.

Os trabalhos futuros passarão por "desdobrar" o modelo proposto num método de implementação de um SGSI, que inclua a identificação e descrição das principais capacidades operacionais e de apoio.

A abordagem destas temáticas necessita de uma visão integrada, multidisciplinar, sistemática e da dedicação de verdadeiros especialistas em permanência nas Organizações.

Agradecimentos

Um agradecimento especial ao Pessoa Dinis e ao João Bessa Pacheco pelas sugestões de simplificação do artigo para uma mais compreensível leitura por leitores não especialistas. Ao João, especialmente pelo contraditório que obrigaram à reflexão e clarificação de alguns dos conceitos e ao Dinis pela discussão sobre a temática da gestão de equipas virtuais.

AS AVALIAÇÕES DE IMPACTO, O ENCARREGADO DE DADOS PESSOAIS E A CERTIFICAÇÃO NO NOVO REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

LUÍS PICA [1]

1 Luís Manuel Pica. Mestre em Direito Tributário e Fiscal pela Escola de Direito da Universidade do Minho; Assistente Convidado do Instituto Politécnico de Beja; Investigador no Lab.- Ubinet do IPBeja. luispica280@gmail.com

RESUMO

O Regulamento Geral de Proteção de Dados Pessoais, aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, é um diploma que foi negociado durante mais de 4 anos e que se erige como um dos mais importantes na história da União Europeia, tendo em vista modernizar e melhorar a regulamentação anterior (Diretiva 95/46/CE, do Parlamento Europeu e do Conselho), aumentado a segurança jurídica que proporciona a execução imediata, geral e uniforme de um regulamento comunitário. O Regulamento Geral de Proteção de Dados Pessoais surge, aqui, como um instrumento legislativo que procura atualizar as normas jurídicas existentes em matéria de proteção de dados pessoais, mas, também, pretende trazer consigo algumas novidades e inovações que a sua predecessora olvidara ou, simplesmente, não fora atualizada com a evolução da sociedade e das novas tecnologias, bem como inovações a nível procedimental e instrumental. São exemplo destas últimas a ascensão das avaliações de impacto, criadas e desenvolvidas no seio do direito anglo-saxónico, e implementadas expressamente no novo Regulamento Geral de Proteção de Dados Pessoais, ou, ainda, a criação de um novo interveniente procedimental no procedimento do tratamento de dados pessoais, como é o Encarregado de Proteção de Dados Pessoais.

Palavras-chave: Proteção de dados; Regulamento Geral Proteção Dados; Avaliação de Impacto; Encarregado Proteção de Dados; Selos e Certificação.

1. INTRODUÇÃO

O Regulamento Geral de Proteção de Dados que entrou em vigor no dia 25 de maio de 2016, e que terá plena aplicação legal em todo o território da União Europeia a 25 de maio de 2018, configura-se como um dos monumentos legislativos de maior importância dos tempos hodiernos, substituindo, até então, o que era o diploma que continha as traves mestres em matéria de tutela de dados pessoais das pessoas singulares, como era a Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

Este Regulamento, apesar das novidades e inovações que um diploma destas características e dimensões não deve abdicar, surge num contexto de continuidade e de evolução da sua predecessora, mantendo certa regulamentação já existente nesta matéria, mas inovando e melhorando aspetos que o legislador considerou como necessários para a concretização do seu verdadeiro escopo. De entre estas inovações destaca-se, do ponto de vista formal, a forma jurídica assumida pela nova legislação, isto é, como um regulamento europeu com as derivações daí advenientes, e, do ponto de vista material, a consagração legal das avaliações de impacto ou a ascensão de uma figura que visa o assessoramento das entidades responsáveis pelo tratamento dos dados e a mediação desta com a autoridade competente.

Como se denota, este novo diploma assume aqui importantes conotações que interessa abordar, mas não deixando de lado parte da regulamentação que existia até então e que se mantém neste novo monumento legislativo.

2. BREVE RESENHA SOBRE O ENQUADRAMENTO LEGAL

A tutela dos dados pessoais das pessoas singulares assumiu, desde muito cedo, uma das preocupações primordiais da então Comunidade Económica Europeia. Iniciou-se esta tutela através da instituição de diretrizes contidas em normas de direito originário, como a existente nos Tratados, Convenções e Cartas de Direitos Fundamentais, desenvolvendo-se, posteriormente, esta regulamentação através de normas de direito derivado,

nomeadamente através da Diretiva 95/46/CE e, mais recentemente, através do Regulamento (UE) 2016/679.Vejamos, assim, as formas de tutela dos dados pessoais.

2.1 - Antecedentes Normativos Europeus

Com o desenvolvimento e a evolução das novas tecnologias o homem viu uma parte da sua privacidade e intimidade, refletida nos dados pessoais, ser tratada de forma automatizada e informatizada. Este tratamento automatizado e a exposição de informação íntima e privada do titular destes dados tornaram possível a ascensão de novos direitos e formas de regulamentação, forçando não só a tutela da intimidade dos sujeitos mas também a busca de garantias que permitissem compatibilizar de forma equitativa a utilização da informática com os vários direitos de que já gozavam estes sujeitos (*v. g.* direito à honra ou o direito ao bom nome)[1]. Foi por isto que nas últimas décadas a proteção dos dados pessoais das pessoas singulares tem vindo a ser alvo de uma constante evolução[2].

Na União Europeia, esta preocupação tem vindo, tendencialmente, a ser marcada pela crescente legislação de normas jurídicas que, na sua génese, tem em vista a tutela destes dados pessoais das pessoas singulares (preocupação imediata), mas também a

1 "*En verdad, el progreso social y el desarrollo tecnológico demandan no sólo protección en la más estricta intimidad del individuo, sino también garantías para asegurar el gobierno de la persona en sus relaciones con terceros"*. Cfr. ANA ISABEL HERRÁN ORTIZ, El Derecho a la protección de datos personales en la sociedad de la información, Cuadernos Desto De Derechos Humanos, N.º26, Universidad de Bilbao, 2002, p.13, disponível em http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf, consultado a última vez em 07/03/2017; LUÍS MANUEL PICA, O direito à autodeterminação informativa dos contribuintes e a proteção dos dados pessoais em matéria tributária, Dissertação Mestrado, Universidade do Minho, Braga, 2016, disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/44452/1/Lu%C3%ADs%20Manuel%20Lopes%20Branco%20Pica.pdf, consultada a última vez em 07/03/2018; JÜRGEN SCHWABE, *Fünfzig Jahre Des Deutschen Bundesverfassungsgerichts Rechtswissenschaft,* Konrad-Adenauer-Stiftung E. V., Berlim, 2005, trad. port. de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Geraldes Ferreira, *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, Fundación Konrad-Adenauer, Oficina Uruguay, Montevideo, 2005.

2 "O progresso constante e acelerado no campo das TIC acarreta novas oportunidades para a sociedade, mas também novos desafios de segurança. A combinação de uma cada vez maior dependência destas, com falhas humanas ou danos intencionais, torna a mitigação dos riscos daí derivados muito mais complicada. Se as novas tecnologias comportam, por um lado, um leque alargado de novas oportunidades para o desenvolvimento da sociedade, por outro lado, também implicam novas vulnerabilidades e novas exigências tanto para a segurança das TIC como para toda a sociedade". Cfr. PETR JIRÁSEK, "Non-It Perspetives Of Cyber Security By An It Professional: Challenges And Future Trends", in Cyberlaw by CIJIC, Edição n.º III, fevereiro, 2017, p.20, disponivel em http://www.cijic.org/wp-content/uploads/2017/02/Cyberlaw-by-CIJIC_edicao-n3.pdf, consultado a última vez em 10/03/2018.

uniformização dessas normas em todo o território da União Europeia com vista à concretização do mercado interno (preocupação mediata).

Como primeira manifestação desta tutela encontramos o preceituado no artigo 8.º da Convenção Europeia dos Direitos do Homem, o qual visa, sobretudo, a tutela da vida privada e familiar, e por ingerência, a tutela dos dados pessoais que integram a esfera mais privada e restrita dos cidadãos[3].

Numa aproximação a uma tutela mais rigorosa e expressa, também o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia[4] dispõe no seu n.º1 que "[t]odas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Acresce o n.º2 do preceituado normativo que "[e]sses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei".

Também a regulamentação normativa originária da União vai neste sentido pois o artigo 16.º do Tratado de Funcionamento da União Europeia veio estatuir que "[t]odas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito", criando-se, assim, condições de base à sua tutela. No que toca à regulamentação normativa secundária na União Europeia, foi pioneira a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, criando um instrumento harmonizador com o desiderato de criar mecanismos uniformes de proteção dos dados pessoais das pessoas singulares na União Europeia, bem como instrumentos de circulação desses mesmos dados pessoais, fomentando, assim, a concretização do mercado interno[5].

3 Sobre esta matéria, Cfr. RITA AMARAL CABRAL, "O Direito à Intimidade da Vida Privada", *in Estudos em Memória do Prof. Doutor Paulo Cunha*, Lisboa, 1989; RABINDRANATH CAPELO DE SOUSA, O Direito Geral de Personalidade, Coimbra Editora, 1995.

4 Sobre a tutela dos dados pessoais na Carta dos Direitos Fundamentais da União Europeia, Cfr. CARLOS RUIZ MIGUEL. "El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Union Europea", *in La Carta de Derechos Fundamentales de la Unión Europea: una perspetiva pluridisciplinar*, Fundación Rei Afonso Henriques, 2003, disponível em http://dialnet.unirioja.es/descarga/articulo/635290.pdf, consultado a última vez em 07/03/2018.

5 Cfr. MANUEL DAVID MASSENO, O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia, 8º Congresso de Direito de Informática e Telecomunicações, setembro 2016, disponível em https://www.academia.edu/31981614/O_novo_Regulamento_Geral_sobre_proteção_de_dados_pessoais_da_União_Europeia?auto=download, consultado a última vez em 12/03/2018.

Estavam assim criadas condições que permitiam uma legislação, entre os Estados-Membros, harmonizada e que criava mecanismos que visavam suprimir os entraves à livre circulação dos dados pessoais, e fomentado a tutela destes no espaço da União Europeia.

2.2 - A Lei Proteção de Dados Pessoais - Lei n.º 67/98, de 26 de outubro de 1998

A transposição para o ordenamento jurídico português da já mencionada Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, foi realizada pela Lei n.º 67/98, de 26 de outubro de 1998, a qual aprovou a Lei de Proteção de Dados Pessoais (doravante denominada pelas siglas "LPDP").

A LPDP procurou expressamente a "proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados", tal como se encontra disposto no primeiro artigo da mencionada Lei. Para além disso, a LPDP veio delimitar as formas de recolha, tratamento, transmissão, registo e conservação dos dados pessoais das pessoas singulares, bem como a criação da entidade independente que visa a fiscalização do cumprimento deste normativo legal (nomeadamente a Comissão Nacional de Proteção de Dados).

Quanto aos princípios norteadores em matéria de proteção dos dados pessoais das pessoas singulares, a LPDP erigiu-se como um diploma de base para os vários ramos do direito em que era necessária a utilização, recolha e conservação destes dados, aplicando-se subsidiariamente às várias relações jurídicas constituídas entre sujeitos de direito[6].

Neste sentido, a LPDP veio consagrar um conjunto de diretrizes fundamentais que determinavam o modo como as entidades responsáveis pela recolha e tratamento dos dados pessoais deviam pautar as suas atuações no âmbito deste procedimento:

a) foi assim com o *princípio da licitude* consagrado na alínea a) do n.º1 do artigo 5.º da LPDP, que obrigava as entidades responsáveis pelo tratamento a recolher e tratar os

6 Foi assim no âmbito dos contratos de consumo celebrados entre consumidores e prestadores de serviços; também em matéria tributária a Administração Tributária e Aduaneira é pautada por este diploma no que toca à recolha e tratamento dos dados pessoais dos contribuintes; em matéria processual, a transmissão de dados pessoais dos executados, no âmbito da ação executiva, como são os dados de vencimento para penhora de vencimentos, deve ser feita em respeito pelo princípio da proporcionalidade e com vista ao estritamente necessário.

dados pessoais em respeito pelo princípio da boa-fé obrigando a que a sua recolha seja conseguida de modo legal e dentro dos ditames legais;

b) também o *princípio da finalidade* teve grande importância nesta matéria pois determinava que a recolha dos dados pessoais fosse concretizada para finalidades específicas e expressamente determinadas, encontrando consagração normativa na alínea b) do n.º1 do artigo 5.º da LPDP;

c) outro dos princípios enformadores, e de grande importância em matéria de proteção de dados pessoais, é o *princípio da exatidão e da qualidade* gizado na alínea d) do n.º1 do artigo 5.º da LPDP, conduzindo, principalmente, a que o responsável pelo tratamento dos dados pessoais deve recolher e tratar as informações cujo teor deve ser exato, correto, completo e atualizado, não sendo permitido o seu tratamento quando estes se afigurem como parciais, incompletos ou fracionados e que por conseguinte induzam em erro;

d) por último, os dados pessoais devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

Relativamente aos princípios fundamentais inerentes ao consentimento do titular dos dados pessoais, veio a LPDP ser de enorme importância em matéria de consentimento dado pela titular destes, sendo o seu tratamento consentido[7] para:

a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido;

b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;

c) Proteção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;

7 Cf. Artigo 6.º da Lei n.º 67/98, de 26 de outubro de 1998.

d) Execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados.

A LPDP procurou ainda instituir mecanismos de circulação de dados pessoais tanto a nível da União Europeia, sendo o princípio geral o de livre circulação dos dados pessoais entre Estados-Membros da União Europeia[8], como a nível internacional, devendo, nestes casos, ser assegurado um nível de proteção adequado, cabendo à Comissão Nacional de Proteção de Dados a decisão se o País em questão cumpre ou não com os níveis de tutela adequados para ser realizada esta transferência.

Por último, foi criada, com a aprovação da Lei n.º 67/98, de 26 de outubro de 1998, a entidade independente na qual era confiada a tarefa de fiscalização das disposições legais ali aprovadas. A já mencionada Comissão Nacional de Proteção de Dados é a autoridade nacional que tem como principal tarefa controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei[9].

2.3 - Regulamento Geral sobre a Proteção de Dados

No dia 25 de janeiro de 2012, a Comissão Europeia apresentou um conjunto de iniciativas de índole legislativa as quais tinham como principal desiderato a reforma do sistema europeu de proteção de dados.

No ato de apresentação da intenção, a Comissária da Justiça e Vice-Presidente da Comissão Europeia, Viviane Reding, realçou a necessidade de reforma[10]. Essa reforma

8 Cf. Artigo 18.º da Lei n.º 67/98, de 26 de outubro de 1998.
9 Cf. Artigo 22º n.º1 da Lei n.º 67/98, de 26 de outubro de 1998.
10 *"Our current data protection rules already contain solid data protection principles. But they were drawn up in 1990 and adopted in 1995, when only 1% of the EU population was using the Internet. In 1995 a 28.8 Kilobytes per*

assentava, principalmente, em dois projetos normativos: a) em primeiro, a Comissão apresentara um Projeto de Regulamento do Parlamento Europeu e do Conselho para a proteção dos cidadãos em relação ao tratamento dos dados pessoais e à livre circulação destes; em segundo, a Comissão apresentou um projeto de Diretiva do Parlamento Europeu e do Conselho sobre a proteção dos cidadão em relação ao tratamento dos dados pessoais pelas autoridades competentes com a finalidade de prevenir, investigar, detetar atos criminais ou executar penas, e sobre a livre transferência desses dados.

As iniciativas da Comissão Europeia comportam uma revisão global do sistema europeu de proteção de dados, tanto num âmbito formal como substantivo. Por um lado, o novo normativo europeu será baseado num diferente instrumento legal (o Regulamento Geral sobre a Proteção de Dados em detrimento da Diretiva 95/46/CE) e, por outro lado, resulta evidente que este novo normativo abordará algumas problemáticas até ao momento não satisfatoriamente resolvidas pelas normas vigentes.

Este Regulamento Geral sobre a Proteção de Dados Pessoais na União Europeia (doravante denominado pelas siglas "RGPD"), aprovado pelo 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, a qual foi transposta no ordenamento jurídico português pela já mencionada Lei n.º67/98, de 26 de outubro de 1998, teve origem num largo processo legislativo.

Este novo instrumento jurídico é o resultado de um longo processo que se pode situar, do ponto de vista institucional, no ano de 2010 quando o Conselho Europeu juntamente com a Comissão Europeia avaliaram o funcionamento dos instrumentos aprovados e que se encontravam em vigor na União sobre a tutela dos dados pessoais,

second modem cost more than 500 euros, Amazon and eBay were still being launched and the founder of Facebook was only 11 years old! It would still be 3 years before the arrival of Google and other household names. But gone are the days of mobile phones the size of bricks and punched card computer programming! Today, just as your computing operating systems and smartphones need regular updates to take new technological developments into account, our data protection rules also needed to be modernised. So we are updating our rules to ensure that they continue to protect individuals in this brave new digital world." Texto de apresentação de Viviane Reding, Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world, June, 2012, disponível em http://europa.eu/rapid/press-release_SPEECH-12-464_en.htm, consultado a última vez

podendo, em caso de ser necessário, apresentar iniciativas com vista a colmatar as deficiências existentes[11] [12].

Neste sentido, tanto o Parlamento Europeu defendeu a ideia de ser criado um regime geral relativo à proteção dos dados pessoais na União Europeia, bem como a Comissão Europeia defendeu a necessidade de garantir o direito fundamental de proteção dos dados pessoais de forma coerente e em consonância com as políticas existentes na União Europeia[13] [14].

Com isto, no dia 27 de janeiro de 2012, a Comissão Europeia elaborou uma proposta de Regulamento relativo à proteção dos dados pessoais das pessoas físicas e à sua circulação no espaço comunitário.

Por fim, em 4 de maio de 2016 foi publicado no Diário Oficial da União Europeia, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, que visava a proteção das pessoas singulares em matéria de tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE.

Este monumento legislativo entrou em vigor no dia 25 de maio de 2016, sendo que existe um período transitório de 2 anos para a sua total aplicação, tendo os responsáveis pelo tratamento dos dados pessoais o mencionado prazo para se adaptarem às novas regras aprovadas, configurando-se estas normas como diretamente aplicáveis sem necessidade dos Estados-Membros as transporem para a ordem jurídica interna, garantindo-se, assim, uma "total"[15] harmonização legislativa em matéria de tutela dos dados pessoais. Destarte, gozam os responsáveis pelo tratamento dos dados pessoais de um período relativamente generoso

11 Cfr. Programa de Estocolmo, "Uma Europa aberta e segura que sirva e proteja os cidadãos", *in* Jornal Oficial C 115 de 4.5.2010, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52010XG0504(01), consultado a última vez em 05/03/2018.

12 Cfr. MANUEL DAVID MASSENO, O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia, … *op. cit.*

13 Cfr. Parecer do Comité Económico e Social Europeu sobre a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da proteção de dados pessoais na União Europeia», *in COM(2010) 609 final] 2011/C 248/21*, disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52011AE0999&from=ES, consultado a última vez em 05/03/2018.

14 Cfr. Resolução do Parlamento Europeu, de 25 de novembro de 2009, sobre a Comunicação da Comissão – Um espaço de liberdade, de segurança e de justiça ao serviço dos cidadãos – Programa de Estocolmo, P7_TA(2009)0090, disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA2009-0090+0+DOC+XML+V0//PT, consultado a última vez em 05/03/2018.

15 Sublinhamos que a aparência de "total harmonização" não é concretizada na sua completa terminologia pois os Estados-Membros gozam de autonomia para legislar sobre determinadas matérias em que o Regulamento assim o permite.

de *vacatio legis* concedido para que estes possam ir preparando e adaptando as suas organizações aos conteúdos das novas normas e, ao mesmo tempo, permitindo aos Estados a atividade legislativa necessária para adequar o sistema jurídico à plena vigência do Regulamento.

Em suma, podemos afirmar que este Regulamento procura, assim, desenvolver a regulamentação jurídica global europeia existente em matéria de proteção de dados já que, por um lado, esta nova regulamentação irá resultar diretamente e imediatamente aplicável por gozar de natureza de regulamento europeu e, por outro lado, irá proporcionar novos direitos aos cidadãos[16].

3. A ESTRATÉGIA PREVENTIVA NO NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: AVALIAÇÃO DE IMPACTO, ENCARREGADO DE PROTEÇÃO DE DADOS, SELOS E CÓDIGOS DE CONDUTA

A era do *Big Data* dificilmente irá encontrar resposta aos riscos que sobrevoam o tratamento dos dados pessoais através (unicamente) de meios repressivos e sancionatórios, ou seja, difícil será admitir que determinado diploma legislativo de tamanha importância tenha como única via de intervenção aquelas situações patológicas da relação jurídica.

Partindo, assim, do pressuposto que o direito melhor tutelado é aquele onde se resolvem, previamente, as vulnerabilidades e se procura tutelar preventivamente os bens jurídicos em questão, o legislador europeu desenhou um conjunto de mecanismos, de natureza preventiva, que tem como desiderato reforçar a tutela dos dados pessoais desde o início do tratamento com vista ao reforço da responsabilização das entidades[17].

16 Cfr. ARTEMI RALLO LOMBARTE, "Hacia un Nuevo Sistema Europeo de Protección de Datos: Las Claves de la Reforma" in UNED. *Revista de Derecho Político* N.º 85, septiembre-diciembre, 2012, pp. 13-56, disponível http://revistas.uned.es/index.php/derechopolitico/article/view/10244/9782, consultado a última vez em 09/03/2018.
17 Cfr. ARTEMI RALLO LOMBARTE, "Hacia un Nuevo Sistema Europeo de Protección de Datos: Las Claves de la Reforma"… *op. cit.*

Em primeiro lugar, o RGPD institui normativamente uma prática preventiva já bastante utilizada nos países de família jurídica Anglo-Saxónica designada como *Privacy Impact Assessment (PIA)*[18], avaliando-se o impacto, em matéria de proteção de dados, sobre o tratamento de determinados tipos de dados pessoais que, pela sua natureza, alcance ou fins, determinem riscos específicos, como poderá ocorrer em situações exemplificativamente previstas no próprio RGPD.

Em segundo lugar, outra das grandes apostas concretizada pelo legislador europeu reside na ascensão de um novo interveniente em matéria de proteção de dados pessoais - já existente em alguns ordenamentos jurídicos como Alemanha ou França -, como é o Encarregado de Proteção de Dados. Este novo interveniente passa a ser obrigatório no organograma de determinada organização, como serão as instituições públicas ou empresas com grande número de trabalhadores. Relevante neste aspeto é o facto de o Encarregado de Proteção de Dados ser uma entidade com competências para se relacionar diretamente com a Comissão Nacional de Proteção de Dados, o público e os interessados, configurando-se como uma entidade que exercerá as suas obrigações de forma independente ao responsável pelo tratamento dos dados pessoais, não podendo receber instruções deste que coloquem em risco a sua isenção. As suas funções assumem-se, assim, em informar e assessorar o responsável pelo tratamento dos dados, instruindo-o sobre as suas obrigações legais e supervisionando as políticas internas de privacidade em respeito pelas garantias de proteção dos dados, desde o desenho à segurança destes, à informação, à notificação de violação, à avaliação de impacto e cooperando com a autoridade de controlo dos dados.

Em terceiro lugar, o legislador europeu manteve o clausulado legal quanto aos códigos de conduta, mas abre outra via de autorregulamentação como são as certificações e os selos com vista a uma exteriorização das competências internas no cumprimento do RGPD.

Vejamos assim com maior precisão de todas estas novas inovações trazidas pelo RGPD em matéria de prevenção na tutela dos dados pessoais das pessoas singulares.

18 Cfr. REHAB ALNEMR, ERDAL CAYIRCI, LORENZO DALLA CORTE, ALEXANDR GARAGA, RONALD LEENES, RODNEY MHUNGU, SIANI PEARSON, CHRIS REED, ANDERSON SANTANA DE OLIVEIRA, DIMITRA STEFANATOU, KATERINA TETRIMIDA AND ASMA VRANAKI, "A Data Protection Impact Assessment Methodology for Cloud", in Springer-Verlag Berlin Heidelberg, 2011, disponível em https://pdfs.semanticscholar.org/5b74/2c82769c026f9c487d4d84d46f1ff86ea061.pdf, consultado a última vez em 10/03/2018.

3.1 - Avaliação de Impacto sobre a Proteção de Dados

A avaliação de impacto sobre a proteção de dados pessoais é uma das principais medidas normativas aprovadas pelo novo RGPD, encontrando-se este instituto ancorado no artigo 35.º do mencionado diploma legal.

Esta técnica de avaliação de riscos no procedimento de tratamento de dados pessoais não é inovação quanto à sua existência pois esta é bastante conceituada e utilizada nos países anglo-saxónicos, sendo esta a sua origem e daí surgindo a designação de PIA's (*Privacy Impact Assessments).* No entanto a sua regulamentação expressa no plano Europeu configura-se como uma das principais novidades deste diploma.

A avaliação de impacto pode definir como um exercício prévio de análise dos riscos que um determinado sistema de informação, produto ou serviço pode ter sobre algum direito fundamental como é o direito à tutela dos dados pessoais, permitindo afrontar eficazmente os riscos identificados mediante a adoção de medidas necessárias para eliminar ou mitigar estes riscos[19]. Sufragando esta opinião a própria Autoridade de trabalho para proteção de dados da União Europeia afirma que "[u]ma AIPD [Avaliação de impacto] é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos (…) Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar conformidade."[20].

Neste sentido dispõe o n.º1 do artigo 35.º do RGPD que "quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas

19 Cfr. Information Comissioner's Office, *Conducting privacy impact assessments code of practice*, 2014, pp.5 e seguintes, disponível em https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf, consultado a última vez em 05/03/2018.

20 Cfr. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 - Documento WP 248 rev.01, abril, 2017, p.4, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf, consultado a última vez em 06/03/2018. (Interpolação nossa).

sobre a proteção de dados pessoais". Ora, daqui podem-se extrair uma série de ilações que merecem reparo e interessa dissecar.

Em primeiro lugar, e como *supra* referido, o procedimento de avaliação de impacto é um **procedimento prévio** ao início do tratamento dos dados pessoais, ocorrendo assim antes do tratamento destes e com fins de análise ao procedimento principal.

Em segundo lugar, esta avaliação de impacto apenas tem lugar quando for utilizada nova tecnologia e o tratamento dos dados pessoais for suscetível de implicar um **elevado risco**[21] [22] para os direitos fundamentais dos titulares dos dados pessoais, competindo à autoridade de controlo (em Portugal a Comissão Nacional de Proteção de Dados) elaborar uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto[23] [24].

Em terceiro lugar, o tratamento tem de ser suscetível de comportar um elevado risco para os **direitos e liberdades das pessoas singulares,** ou seja, todos os direitos que visem a tutela direta dos dados pessoais e da privacidade do seu titular mas, também, todos os direitos indiretos como serão os direitos de liberdade de circulação, liberdade de expressão ou liberdade de pensamento.

Com esta análise de impacto consegue-se desde logo identificar os possíveis riscos para a proteção dos dados pessoais dos afetados e a valorização da probabilidade de ocorrerem, bem como os danos que causariam se se materializassem. Feita esta análise é possível, previamente, determinar as medidas que devem ser implementadas a fim de

21 Apesar de o RGPD não especificar o que deve ser entendido por "elevado risco", podemos indicar, segundo também vários documentos emitidos pelas autoridades de proteção de dados da União Europeia, como sendo atividades de perigosidade para os direitos dos titulares dos dados pessoais, as seguintes atividades: a) tratamento que avaliem aspetos pessoais relativos a pessoas físicas, baseados em tratamento automatizado de dados que produzam efeitos jurídicos na esfera jurídica destes, como poderá ser a decisão de obter um crédito bancário baseado unicamente no processamento automático feito por um programa de computador; b) tratamento de dados em setores de natureza vulnerável, como poderá ser o setor laboral; c) tratamento de dados sensíveis como são os dados pessoais que revelem as opiniões políticas e religiosas, o tratamento de dados genéticos, os dados biométricos; a monitorização sistemática em que existem controlos de vigilância; e as transferências internacionais de dados para o espaço externo à União Europeia.

22 Cfr. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) … *op. cit.*, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf, consultado a última vez em 06/03/2018.

23 Cf. Artigo 35.º n.º4 do RGPD.

24 No entanto pode a Comissão Nacional de Proteção de Dados identificar negativamente os tipos de operações de tratamento em relação às quais não é obrigatória a elaboração de uma avaliação de impacto, conforme preceitua o n.º5 do artigo 35.º do RGPD.

eliminar ou mitigar os riscos detetados, permitindo adotá-los no tratamento dos dados pessoais a fim de concretizar a tutela dos direitos fundamentais dos titulares destes[25].

Como veremos *infra*, uma das principais novidades que o novo RGPD trouxe face à Diretiva 95/46/CE foi a criação de uma "entidade interna" existente na organização do responsável pelo tratamento dos dados pessoais, o qual tem como tarefa primordial zelar pelo cumprimento das normativas relacionadas com o tratamento destes. Esta "entidade" foi designada pelo legislador como *encarregado da proteção de dados*, passando a entidade de controlo a ter um papel mais residual intervindo, principalmente, nas situações patológicas da relação jurídica constituída entre o responsável pelo tratamento dos dados pessoais e o seu titular.

Uma das principais tarefas do encarregado da proteção de dados é, segundo o conceituado na alínea c) do n.º1 do artigo 39.º do RGPD, o de prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do n.º2 do artigo 35.º. Deste modo, sempre que a entidade responsável pelo tratamento dos dados pessoais possua alguém a exercer as tarefas inerentes à atividade de encarregado da proteção de dados, fica este obrigado a emitir parecer a sobre esta avaliação de impacto.

No entanto, esta avaliação de impacto resulta obrigatória quando o tratamento dos dados pessoais tenha como objeto a avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, devendo este ser baseado no tratamento automatizado, incluindo definição de perfis, tendo como principal objetivo a tomada de decisões que produzam efeitos jurídicos na esfera do titular destes dados pessoais; esta avaliação de impacto configura-se, também, como obrigatória quando haja operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º, e ainda quanto aos dados pessoais relativos a menores; por último é também obrigatório proceder a esta avaliação de impacto nos casos de controlo sistemático de zonas acessíveis ao público em grande escala, ou seja, quando seja utilizados meios tecnológicos considerados invasivos da privacidade como serão, a título

25 Neste sentido afirma o considerando 84 do RGPD que "[o]s resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento".

meramente exemplificativo, vigilância a grande escala, geolocalização, vigilância eletrónica, técnicas genéticas, etc.[26].

Em suma pode-se referir que as entidades obrigadas a realizar este procedimento serão, nomeadamente: as empresas de segurança privada, vigilância e controlo, hospitais e clínicas, escolas, empresas envolvidas no e-commerce, farmácias e comercializadores de energia.

A avaliação de impacto a que se refere o artigo 35.º do RGPD deve conter uma série de elementos, indispensáveis e irrenunciáveis, pois como refere o n.º7 do citado preceito legal deve esta conter, *pelo menos:* uma descrição das operações de tratamento que pretende efetuar e qual a sua finalidade, bem como os interesses do responsável pelo tratamento, se o mesmo não se vislumbrar da finalidade pretendida com o tratamento; deve incluir, também, uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos pretendidos, pois caso os mesmos se configurem como desnecessários e desproporcionais não haverá necessidade deste tratamento ser efetuado da forma descrita e pretendida; uma avaliação sobre os eventuais riscos e ofensas aos direitos fundamentais dos titulares dos dados pessoais em virtude das operações realizadas no tratamento destes; por último é também obrigatório que a avaliação de impacto inclua as medidas reparadoras, preventivas, medidas de segurança e procedimentos que visem assegurar a proteção dos dados pessoais tratados a fim de comprovar a total legitimação entre a operação realizada e o cumprimento das normas presentes no Regulamento Geral.

A avaliação de impacto pode ser considerada como um projeto sobre o procedimento de tratamento dos dados pessoais na medida em que o responsável pelo tratamento dos dados pessoais pode efetuar um estudo prévio sobre estas operações a fim de verificar se os mesmos estão em conformidade com o resultado obtido na avaliação de impacto realizada antes do inicio destas operações[27].

Daqui podemos encontrar duas situações diversas: ou o resultado da avaliação de impacto é positivo e o tratamento e operações dos dados pessoais não resulta na ofensa de qualquer direito fundamental dos seus titulares; ou, pelo contrário, da avaliação de

26 Cf. Artigo 35.º n.º3 do RGPD.
27 Cf. Artigo 35.º n.º11 do RGPD.

impacto resulta que as operações a realizar colocam em risco a esfera jurídica do titular destes dados pessoais. Na primeira situação fácil é denotar que, em nada violando o disposto no Regulamento Geral, pode o tratamento ter lugar sem qualquer intervenção de terceiros ou medidas que atenuem ou afastem possíveis riscos aos direitos fundamentais dos titulares dos dados pessoais. Na segunda situação, e havendo já riscos identificados pela avaliação de impacto na ausência de medidas que afastam ou atenuem o risco, deve o responsável pelo tratamento consultar, previamente às operações de tratamento, a entidade de controlo (como referido, em Portugal a Comissão Nacional de Proteção de Dados) devendo comunicar-lhe quem é o responsável pelo tratamento, as finalidades e os meios de tratamento previstos, as medidas e garantias previstas para salvaguardar os direitos e liberdades dos titulares dos dados pessoais, os contactos do encarregado dos dados pessoais (caso este exista na entidade responsável pelo tratamento), o resultado da avaliação de impacto e, ainda, todas as informações que a entidade de controlo venha a solicitar[28].

A *ratio essendi* a esta consulta prévia à autoridade de controlo não é mais que a de salvaguardar os direitos e liberdades dos titulares dos dados pessoais, já que se este tratamento e operações têm subjacentes riscos para estes, não podem estas operações ser realizadas sem uma prévia consulta à autoridade de controlo.

Deste modo é nossa opinião que esta consulta prévia à autoridade de controlo apenas deve ter lugar quando as operações de tratamento resultem num risco para os direitos fundamentais dos titulares dos dados e não existam medidas que afastem ou atenuem este risco, pois caso existam e possam ser implementadas, não será necessária a consulta e intervenção da autoridade de controlo. Neste sentido parece apontar o próprio RGPD quando dispõe que "[s]empre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais".

Por último, é importante referir a importância deste procedimento para as entidades responsáveis pelo tratamento dos dados pessoais pois, como se encontra expresso na

28 Cf. Artigo 36.º n.º1 e n.º3 do RGPD.

alínea a) do n.º4 do artigo 83.º do RGPD, a não realização da avaliação de impacto - quando devida -, a não conformidade com os requisitos de uma Avaliação de impacto e a realização de forma incorreta de uma avaliação de impacto pode conduzir à imposição de coimas pela autoridade de controlo competente, encontrando-se classificada como uma infração punível com coima até até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

3.2 - O Encarregado da Proteção dos Dados (*Data Protection Officer)*

O novo RGPD traz uma alteração substancial no paradigma das relações jurídicas instituídas entre o responsável pelo tratamento dos dados pessoais e a entidade responsável pelo cumprimento da regulamentação legal vigente nesta matéria. Até à aprovação do RGPD pode-se afirmar que o sistema vigente é um sistema de heterorregulação, passando com a aprovação e entrada em vigor do mesmo a ter um sistema de autorregulação onde as entidades responsáveis pelo tratamento são obrigadas a comprovar a utilização do RGPD à entidade que fiscaliza. Passamos, assim, a ter uma entidade fiscalizadora num papel mais passivo e o qual é chamado a intervir nas situações patológicas da relação jurídica.

Mas para haver autorregulação pelas entidades, ou seja, nas quais estas interpretam e adaptam os seus recursos e meios à legislação em vigor, deve existir alguém com competência material para o fazer. Neste desiderato, e sendo uma das grandes inovações trazidas pela publicação e entrada em vigor do novo RGPD, surge a figura do Encarregado da Proteção dos Dados, ou como comummente designado, *Data Protection Officer (DPO).*

A figura do encarregado da proteção dos dados encontra-se ancorada nos artigos 37.º e seguintes do RGPD, como a entidade responsável pela proteção, gestão e tratamento dos dados de uma empresa ou organização, sendo que as suas principais tarefas podem ser, entre outras não previstas no RGPD, as elencadas no n.º1 do artigo 39.º do RGPD, nomeadamente:

a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controlar a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º;

d) Cooperar com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

A sua principal tarefa consubstancia-se em informar ao responsável pelo tratamento dos dados sobre os aspetos legais e práticos ligados a estas operações, supervisionando que se apliquem as normas jurídicas aprovadas no presente Regulamento, zelando, assim, pelo seu cumprimento. O encarregado da proteção dos dados surge aqui como uma figura de transcendental importância no novo paradigma subjacente à relação entre as autoridades de controlo e as entidades responsáveis pelo tratamento dos dados pessoais, pois, com a entrada em vigor do novo Regulamento, as autoridades de controlo deverão atuar apenas nas situações patológicas da relação jurídica, devendo as entidades responsáveis pelo tratamento dos dados assegurar o cumprimento estrito do disposto no citado Regulamento, sob pena de incorrerem em pesadas sanções.

Deste modo poderemos identificar como funções do encarregado da proteção dos dados, nomeadamente: assessorar os responsáveis pelo tratamento dos dados pessoais e os trabalhadores destas sobre as obrigações legais que devem cumprir; supervisionar as tarefas que se encontram subjacente ao tratamento dos dados pessoais; avaliar o impacto das ações de risco elevado para os direitos fundamentais dos titulares dos dados pessoais;

e, ainda, colaborar com a Comissão Nacional de Proteção de Dados trabalhando como intermediário entre o responsável pelo tratamento dos dados pessoais e a autoridade de controlo[29].

No entanto, a existência do encarregado de proteção dos dados no organograma apenas é obrigatória quando preenchidos alguns requisitos previstos legalmente, os quais não podem aqui ser entendidos como cumulativos. Assim, é obrigatória a designação de um encarregado de proteção de dados quando este tratamento for efetuado por uma autoridade ou organismo público (*v.g.* Autoridade Tributária e Aduaneira; Câmaras Municipais), quando as atividades principais do responsável pelo tratamento subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala[30], ou, então, quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados[31].

Dispõe o n.º4 do artigo 37.º do RGPD que "[e]m casos diferentes dos visados no n.º 1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um encarregado da proteção de dados". Portanto, entidades ou atividades indicadas pelo legislador podem, mediante lei estadual aprovada pelo Estado-Membro, ser sujeitas à designação de um encarregado de proteção de dados mesmo que não indicadas neste n.º1 do artigo 37.º do RGPD.

Questão que urge ainda analisar é saber quem pode ser designado para encarregado de proteção de dados?

O RGPD não concreta quem é que deve assumir esta posição, no entanto, como se descortina do n.º5 e n.º6 do artigo 37.º do RGPD, o encarregado da proteção de dados é designado e/ou contratado segundo a sua capacidade para exercer as competências fixadas pelo regulamento e, concretamente, pelos seus conhecimentos em matéria de direito e

29 Cf. Artigo 39.º do RGPD.
30 Aqui devem apenas ser entendidas as atividades primárias e principais praticadas por estas entidades, pelo que não se incluem as entidades que pratiquem estas atividades a título secundário à sua atividade central.
31 Cf. Artigo 37.º n.º1 do RGPD.

proteção de dados. Para desempenhar esta função, juristas ou pessoas com sólidos conhecimentos sobre o RGPD são de enorme importância para assumirem estes cargos nas empresas e entidades responsáveis por este tratamento, não sendo, pelo momento, necessária qualquer creditação aprovada pela Comissão Nacional de Proteção de Dados para designar determinada pessoa como "competente" para exercer este cargo, pelo que basta a competência da pessoa para exercer esta tarefa.

Este encarregado da proteção de dados surge como uma *figura híbrida* nesta relação jurídica pois, por um lado, surge no organograma da entidade responsável pelo tratamento e, pelo outro, as suas funções assemelham-se como intermediária e um "agente" da Comissão Nacional de Proteção de Dados no cumprimento das normas jurídicas aprovadas no Regulamento. Sufragando esta ideia parece apontar o n.º1 e n.º3 do artigo 38.º do RGPD quando expressamente indica que "[o] responsável pelo tratamento e o subcontratante asseguram que [o encarregado] da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções", acrescentando ainda o ponto 97 das considerações preambulares que "[e]stes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com *independência*".

Pelo exposto, pode-se vislumbrar que o encarregado da proteção dos dados é aqui um sujeito procedimental que goza de certa autonomia face ao responsável pelo tratamento dos dados pessoais, pois não pode aqui ser penalizado pelos atos deste, nem pode ser induzido, conduzido ou influenciado nos atos próprios das suas funções. Fácil é assim de denotar que a *ratio* desta norma surge na senda que a sua função assume-se como um sujeito que tem como principal desiderato o cumprimento das normas constantes do RGPD, configurando-se como uma ponte de interligação entre a entidade responsável pelo tratamento dos dados e a Comissão Nacional de Proteção de Dados, pelo que a influência por uma destas entidades colocaria em causa esta posição de "intermediário" e por conseguinte o bom cumprimento das normas presentes no Regulamento.

3.3 - Códigos de Conduta

Os códigos de conduta constituem uma ferramenta de natureza transversal a todos os ramos do Direito, configurando-se como um instrumento similar ao movimento existente com a codificação que originaram os atuais códigos tipo existentes nos ordenamentos jurídicos.

Em matéria de proteção de dados pessoais, os códigos de conduta surgem no novo regulamento como um instrumento essencial para as organizações responsáveis pelo tratamento destes[32] [33]. Neste sentido, aponta o ponto 98 das considerações preambulares que "[a]s associações ou outras entidades que representem categorias de responsáveis pelo tratamento ou de subcontratantes deverão ser incentivadas a elaborar códigos de conduta, no respeito do presente regulamento, com vista a facilitar a sua aplicação efetiva, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas. Esses códigos de conduta poderão nomeadamente regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares".

Deste modo, o RGPD reconhece a aprovação de códigos de conduta pois como refere no n.º1 do artigo 40.º do citado diploma, "[o]s Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas". Mas não apenas estas tem legitimidade legal para criar códigos de conduta pois conforme preceitua o n.º2 do citado normativo legal, as associações e outros organismos representativos podem elaborar, modificar ou ampliar

32 A existência de Código de Conduta em matéria de proteção de dados pessoais não é uma novidade pois, a própria Lei n.º67/98 de 26 de outubro, já previa a existência destes códigos conforme preceitua o artigo 32.º do citado diploma legal.

33 Um dos melhores exemplos dos códigos de conduta aprovados e que tem em vista a uniformização das práticas de determinada atividade relacionada com a proteção de dados em consonância com o disposto no RGPD, é o Código de Conduta CISPE (*Cloud Infrastructure Service Providers in Europ*e), aprovado para os Provedores de Serviço de Infraestrutura em Nuvem, e que tem como finalidade uniformizar as normas tendentes a esta atividade. A versão original deste Código de Conduta pode ser consultado na íntegra através de https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct27-January2017-corrected-march20.pdf, consultado a última vez em 05/03/2018.

um código de conduta com a finalidade de o especificar a e adaptar ao próprio Regulamento.

Neste sentido, o próprio RGPD exemplifica alguns dos parâmetros que os códigos de conduta podem regular, nomeadamente:

"a) O tratamento equitativo e transparente; b) Os legítimos interesses dos responsáveis pelo tratamento em contextos específicos; c) A recolha de dados pessoais; d) A pseudonimização dos dados pessoais; e) A informação prestada ao público e aos titulares dos dados; f) O exercício dos direitos dos titulares dos dados; g) As informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido; h) As medidas e procedimentos a que se referem os artigos 24.º e 25.º e as medidas destinadas a garantir a segurança do tratamento referidas no artigo 30.º; i) A notificação de violações de dados pessoais às autoridades de controlo e a comunicação dessas violações de dados pessoais aos titulares dos dados; j) A transferência de dados pessoais para países terceiros ou organizações internacionais; ou, k) As ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados em relação ao tratamento, sem prejuízo dos direitos dos titulares dos dados nos termos dos artigos 77.º e 79.º."

Esta alteração é realizada mediante comunicação à Comissão Nacional de Proteção de Dados, apresentando um projeto de código para que esta o análise e verifique a sua conformidade com o disposto no RGPD.

Após análise desse projeto, a Comissão Nacional de Proteção de Dados emite parecer sobre a conformidade do projeto de código, podendo, aqui, haver duas situações que merecem reparo: caso a atividade de tratamento não esteja relacionada com vários Estados-Membros e o projeto de código esteja em conformidade com as normas presentes no RGPD, o mesmo será publicado e registado para aplicação; em caso da atividade estar ligada a vários Estados-Membros, não pode a Comissão Nacional de Proteção de Dados aprovar e registar o código de conduta de imediato, sem antes de a aprovação ser apresentado o projeto do código, a alteração ou o aditamento, pelo procedimento referido no artigo 63.º, ao Comité, que emite um parecer sobre a conformidade do projeto de

código de conduta, ou da alteração ou do aditamento, com o disposto no RGPD, remetendo esse parecer para a Comissão, nos termos do n.º8 do artigo 40.º do RGPD.

A *ratio* subjacente a esta norma que impõe a intervenção das entidades Europeias encontra-se relacionada com a necessidade imperativa de a proteção de dados pessoais das pessoas físicas merecer grande importância e uniformidade na União Europeia, pelo que se determinada atividade é comum a vários Estados-Membros, é necessário, e proveitoso, que seja de aplicar em todos esses Estados-Membros e setores da atividade interligados entre si, com o intuito de quebrar a barreira entre países e fomentar a livre circulação na União Europeia.

Neste sentido parece apontar o n.º9 do artigo 40.º do RGPD, pois o mesmo indica que a Comissão pode, através de atos de execução, decidir que determinado código de conduta, aprovado nos termos *supra* expostos, seja aplicável em todos os Estados-Membros, e por conseguinte aplicado de modo geral na União Europeia.

3.4 - Certificação, Selos e Marcas

O procedimento de certificação das operações de tratamento de dados pessoais encontra-se ancorada no novo RGPD, nomeadamente nos artigos 42.º e seguintes deste diploma legal.

A existência de certificações, selos e marcas de procedimentos de tratamento de dados pessoais tem como desiderato demonstrar que determinada operação de tratamento de dados cumpre com o disposto no RGPD. Como ponto de partida, têm-se em vista que o "Selo Europeu de Proteção de Dados" visa criar confiança entre os interessados, consumidores e titulares dos dados pessoais, dotando-os de maior certeza e rapidez na hora de analisar os produtos e serviços correspondentes.

Neste sentido dispõe o n.º1 do artigo 42.º do RGPD que "[o]s Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o

presente regulamento". Pode-se assim afirmar que os selos, marcas e certificação de procedimentos consistem numa forma de atribuição de um "distintivo" que qualifica determinado procedimento, ou operação que envolva o tratamento de dados pessoais, como cumprindo os pressupostos do presente Regulamento em matéria de tutela dos direitos fundamentais dos titulares dos dados pessoais. Configuram-se, assim, como um mecanismo que visa demonstrar o adequado cumprimento do RGPD, por parte dos responsáveis pelo tratamento dos dados pessoais, proporcionando garantias adequadas para as transferências internacionais de dados tendo em conta as características e necessidades específicas dos diferentes setores de tratamento e âmbitos sectoriais.

Sendo como um distintivo que atribuí qualidade à operação em causa, fácil é de denotar que esta atribuição de certificação só pode ser voluntária, podendo o responsável por estas operações, livremente, optar sobre se quer atribuir uma maior publicidade aos consumidores relativamente a estas, ou pelo contrário não a pretende publicitar. Note-se que, como mecanismo que visa exteriorizar a qualidade de determinado tratamento, esta certificação apenas pode ter caráter temporal pois os métodos de tratamento e a tecnologia utilizada evoluem constantemente, pelo que atribuir certificados, marcas e selos vitalícios a procedimentos e operações em que é utilizada tecnologia avançada seria esvaziar o seu conteúdo racional e lógico. Deste modo, estes certificados, marcas e selos apenas são atribuídos por um período máximo de 3 anos, renováveis pelo mesmo prazo caso se verifiquem as condições que deram origem à atribuição da certificação inicial. No entanto, pode esta certificação ser retirada à entidade responsável pelo tratamento dos dados se os requisitos para a certificação não estiverem ou tiverem deixados de estar reunidos[34].

Para levar a bom porto este procedimento de certificação, o Comité recolhe todos os procedimentos e todos os selos e marcas de proteção de dados aprovados num registo e disponibiliza-os ao público por todos os meios adequados, publicitando-os de modo a comprovar a veracidade dos mesmos e a sua creditação face às entidades que delas disponham[35].

Apesar de a regra em matéria de competência legal para atribuição desta certificação, serem, conforme preceitua o artigo 42.º do RGPD, os Estados-Membros, as autoridades de controlo, o Comité e a Comissão, pode ser atribuído a determinados órgãos

34 Cf. Artigo 42.º n.º3 e n.º7 do RGPD.
35 Cf. Artigo 42.º n.º8 do RGPD.

a competência para atribuição destes certificados, sempre e quando estas tenham um nível adequado de conhecimento em matéria de proteção de dados.

Esta creditação pode ser realizada pela Comissão Nacional de Proteção de Dados, ou pelo organismo nacional de acreditação, designado nos termos do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, em conformidade com a norma EN-ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo, conforme se encontra ancorado no n.º1 do artigo 43.º do RGPD.

Mas para esta acreditação poder ser concretizada, haverá este organismo de certificação de demonstrar, à Comissão Nacional de Proteção de Dados, a sua independência e competência em relação ao objeto da certificação; deverá de comprometer-se a respeitar os critérios de certificação aprovados pela Comissão Nacional de Proteção de Dados; deverá estabelecer procedimentos para emitir, rever e retirar certificações; haverá de estabelecer procedimentos e estruturas para tratar reclamações relativas a infração da certificação; e demonstrar perante a Comissão Nacional de Proteção de Dados que as suas funções e objetivos não dão azo a qualquer conflito de interesses[36]. Esta acreditação do organismo de certificação é realizada por um máximo de cinco anos e pode ser renovado pelas mesmas condições[37], podendo também ser revogada se as condições para a acreditação não estiverem ou tiverem deixado de estar reunidas, ou se as medidas tomadas pelo organismo de certificação violarem o presente no RGPD[38].

Sendo concedida, ou revogada determinada certificação, deve o organismo responsável por esta certificação fornecer à Comissão Nacional de Proteção de Dados os motivos que levaram à concessão ou revogação da certificação solicitada.

Com este ato de acreditação a determinados organismos concede-se uma faculdade de "delegação" das competências previstas na alínea n) do n.º1 do artigo 57.º do RGPD, para organismos terceiros que, no âmbito da atividade, estão familiarizados com a matéria de tratamento e proteção de dados pessoais, passando estas a exercer estas competências que, em regra e à partida, estão na esfera jurídica da Comissão Nacional de Proteção de Dados.

36 Cf. Artigo 43.º n.º2 do RGPD.
37 Cf. Artigo 43.º n.º4 *in fine* do RGPD.
38 Cf. Artigo 43.º n.º7 do RGPD.

4. CONCLUSÃO

Decorridos mais de 20 anos sobre o primeiro monumento legislativo europeu derivado em matéria de proteção de dados pessoais, o novo RGPD aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, surge como uma oportunidade para o legislador europeu avançar e evoluir no seguimento da evolução das novas tecnologias e dos desafios que estas afrontam para a tutela dos dados privados e íntimos das pessoas singulares.

Com o fim de chegar a este desiderato, o legislador instituiu um conjunto de meios que permitem, de forma mais eficiente e uniforme, a aproximação a este objetivo pretendido. Do ponto de vista formal, através da regulamentação em forma de regulamento europeu, procura-se (e consegue-se) aplicar de forma uniforme e sem necessidade de transposição interna as mesmas normas jurídicas em todos os Estados-Membros da União Europeia, deixando de haver certas disparidades que naturalmente existem quando o diploma existente deriva de uma Diretiva; do ponto de vista material procurou-se instituir novas formas de regulamentação, de natureza preventiva, com vista a responsabilizar os responsáveis pelo tratamento dos dados pessoais e a reforçar a tutela destes dados antes da ocorrência de riscos e violações dos mesmos.

O êxito desta nova estratégia de regulamentação desenhada pelo RGPD irá depender da sua eficácia e, em consequência, credibilidade na garantia efetiva do direito à proteção dos dados pessoais, mas certo é que a União Europeia, com quase duas décadas de experiência nesta matéria, conseguiu com este novo Regulamento complementar os sistema jurídico instituído, criando instrumentos alternativos proactivos que completam o desenho original e que dão melhor resposta ao objeto final pretendido, que mais não é o da tutela dos dados pessoais. Com isto procurou-se combinar instrumentos de regulamentação preventiva e repressiva, com o único objetivo de concretizar o desiderato essencial pretendido.

REFERÊNCIAS CITADAS

- ALNEMR, REHAB, *et al.*, "*A Data Protection Impact Assessment Methodology for Cloud"*, in Springer-Verlag Berlin Heidelberg, 2011, disponível em https://pdfs.semanticscholar.org/5b74/2c82769c026f9c487d4d84d46f1ff86ea061.pdf;

- CABRAL, RITA AMARAL, "O Direito à Intimidade da Vida Privada", *in Estudos em Memória do Prof. Doutor Paulo Cunha*, Lisboa, 1989;

- HERRÁN ORTIZ, ANA ISABEL, *El Derecho a la protección de datos personales en la sociedad de la información, Cuadernos Desto De Derechos Humanos*, N.º26, Universidad de Bilbao, 2002, disponível em http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf;

- JIRÁSEK, PETR, "*Non-It Perspetives Of Cyber Security By An It Professional: Challenges And Future Trends*", *in Cyberlaw by CIJIC, Edição n.º III*, fevereiro, 2017, Disponível em http://www.cijic.org/wp-content/uploads/2017/02/Cyberlaw-by-CIJIC_edicao-n3.pdf;

- MANUEL DAVID MASSENO, O novo Regulamento Geral sobre proteção de dados pessoais da União Europeia, 8º Congresso de Direito de Informática e Telecomunicações, setembro 2016, disponível em https://www.academia.edu/31981614/O_novo_Regulamento_Geral_sobre_proteção_de_dados_pessoais_da_União_Europeia?auto=download;

- PICA, LUÍS MANUEL, O direito à autodeterminação informativa dos contribuintes e a proteção dos dados pessoais em matéria tributária, Dissertação Mestrado, Universidade do Minho, Braga, 2016, disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/44452/1/Lu%C3%ADs%20Manuel%20Lopes%20Branco%20Pica.pdf;

- RALLO LOMBARTE, ARTEMI, "*Hacia un Nuevo Sistema Europeo de Protección de Datos: Las Claves de la Reforma*" in *UNED. Revista de Derecho Político* N.º 85, septiembre-diciembre, 2012, disponível http://revistas.uned.es/index.php/derechopolitico/article/view/10244/9782;

- RUIZ MIGUEL, CARLOS, "*El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Union Europea*", *in La Carta de Derechos Fundamentales de la Unión Europea: una perspetiva pluridisciplinar*, Fundación Rei Afonso Henriques, 2003, disponível em http://dialnet.unirioja.es/descarga/articulo/635290.pdf;

- SCHWABE, JÜRGEN, *Fünfzig Jahre Des Deutschen Bundesverfassungsgerichts Rechtswissenschaft*, Konrad-Adenauer-Stiftung E. V., Berlim, 2005, trad. port. de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Geraldes Ferreira, *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, Fundación Konrad-Adenauer, Oficina Uruguay, Montevideo, 2005;

- SOUSA, RABINDRANATH CAPELO DE, O Direito Geral de Personalidade, Coimbra Editora, 1995;

VEÍCULOS AUTÓNOMOS E "INTELIGENTES" PERANTE CONFLITOS DE INTERESSES: UMA VISÃO A PARTIR DO DIREITO DE NECESSIDADE JURÍDICO-PENAL

PEDRO MIGUEL FREITAS [1]

1 Doutor em Direito. Docente universitário. Contato: pedrofernandesfreitas@gmail.com.

RESUMO

Partindo da análise de uma figura jurídico-penal como o direito de necessidade previsto no artigo 34.º do Código Penal Português, pretende-se identificar alguns nós problemáticos que envolvem o fabrico, programação e uso de veículos autónomos. Embora encerrem benefícios perfeitamente identificáveis, o desenvolvimento e implementação de veículos autónomos deve tomar em consideração a possível necessidade de antecipação de dilemas éticos de solução complexa e questionável.

Palavras-Chave: direito de necessidade, interesses jurídicos, veículos autónomos, inteligência artificial.

1. CONSIDERAÇÕES INTRODUTÓRIAS

Começamos este artigo por dizer aquilo que não é, ou melhor, aquilo que não constitui o seu objeto de análise. Embora o tópico da responsabilidade jurídico-penal de agentes de *software* esteja cada vez mais em cima da mesa, e sobre o qual nos debruçámos aliás numa outra ocasião[1], não pretendemos com os apontamentos que se seguirão analisar em que medida poderão preencher-se, *de iure condendo*, os requisitos dogmáticos de uma responsabilidade jurídico-penal e eventuais consequências jurídicas aplicáveis a agentes de *software*. Repare-se. Na doutrina internacional a questão já se coloca, havendo mesmo quem proponha possíveis sanções jurídico-penais aplicáveis a agentes de *software.* Dir-se-á, e com mediana razão, que, no momento atual, tais estudos não passam de meros exercícios especulativos. De acordo. Temos dúvidas, porém, é que estes exercícios especulativos – se assim os quisermos designar – não possam encontrar espaço e razão de ser quer no Direito Penal, quer no seu campo de excelência, a Filosofia. Ademais, se algo há que podemos concluir da velocidade vertiginosa de criação e desenvolvimento das novas tecnologias é que não podemos antecipar com certeza absoluta o que iremos experienciar nas próximas décadas[2].

A inteligência artificial está a dar os primeiros passos de um caminho que poderá revelar-se completamente revolucionário na vivência humana. Contém em si o potencial capaz de pôr em crise o que temos por adquirido e, desse modo, metamorfosear os traços caraterizadores dos fundamentos em que assenta a vida pessoal e comunitária.

Como não podia deixar de ser, as novas tecnologias e a inteligência artificial constituem *um topoi* a que o Direito não pode nem deve olvidar. Mas a criação de normas jurídicas, a sua interpretação e a sua aplicação demandam do legislador e intérprete um tempo próprios que se compadecem mal com fenómenos de grande volatilidade. No caso da inteligência artificial isto é particularmente visível. A sua

1 FREITAS, Pedro Miguel, ANDRADE, Francisco e NOVAIS, Paulo, "Criminal Liability of Autonomous Agents: from the unthinkable to the plausible", in Pompeu Casanovas et al (Eds.), *AICOL IV/V 2013, LNAI 8929*, Springer, 2014, pp. 145-156.

2 Há pouquíssimo tempo foi notícia o atropelamento mortal no estado do Arizona em que esteve envolvido um carro que circulava de forma autónoma, ainda que no seu interior se encontrasse um condutor. Cf. https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe.

evolução tem sido realizada a uma velocidade incrível e dispersa pelos mais diversos domínios, desde os robots, passando pelos veículos autónomos até aos mercados financeiros ou algoritmos de análise da enorme quantidade de dados produzidos ininterruptamente a que se convencionou apelidar *Big Data*.

Não é por isso particularmente surpreendente que as poucas iniciativas legislativas surjam timidamente, de modo fragmentário e compartimentado. De facto, não se descobre neste domínio uma estratégia jurídica integrada. Alguns poderão mencionar a Proposta de Resolução do Parlamento Europeu que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica 2015/2103 (INL), adotada no início do ano passado[3]. Nos seus considerandos iniciais afirmava-se que "é necessário um conjunto de normas que rejam, em especial, a responsabilidade, a transparência e a prestação de contas e traduzam os valores universais intrinsecamente europeus e humanísticos que caracterizam o contributo da Europa para a sociedade; que as normas não devem afetar o processo de investigação, inovação e desenvolvimento na área da robótica". Acrescentava-se que "a União pode desempenhar um papel essencial no estabelecimento de princípios éticos básicos a respeitar no desenvolvimento, na programação e na utilização de robôs e de IA, bem como na integração desses princípios nos regulamentos e nos códigos de conduta da União, com o objetivo de moldar a revolução tecnológica, de modo a que sirva a humanidade e a que as vantagens da robótica avançada e da IA sejam amplamente partilhadas, evitando, tanto quanto possível, potenciais perigos".

Tratou-se de uma proposta notável a vários níveis. Reconheceu a insuficiência do atual quadro normativo para lidar de modo adequado com a atuação de robots ou agentes de *software* que possuam um grau de autonomia e autoaprendizagem tais que dispensam a intervenção humana. O Parlamento Europeu equacionou mesmo, ainda que de forma muito subtil, a possibilidade de um rearranjo da dogmática tradicional do direito civil, quando dizia que "a autonomia dos robôs suscita a questão da sua natureza à luz das categorias jurídicas existentes ou se deve ser criada uma nova categoria, com características e implicações próprias". Recomendou ainda à Comissão que, havendo um futuro instrumento legislativo nesta matéria, deveria ser analisada e considerada a

3 Cf. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//PT#title1.

possibilidade de criação de um estatuto jurídico para os robôs com um grau de autonomia e independência avançado que lhes concedesse "personalidade eletrónica", com a qual seriam responsáveis pela reparação de danos causados com a sua atuação.

Um dos fundamentos para esta nova figura da personalidade eletrónica residiria, se bem compreendemos a proposta, no reconhecimento do impacto atual da robótica e inteligência artificial na sociedade, dado que "os robôs de hoje conseguem efetuar atividades que, regra geral, costumavam ser exclusivamente realizadas por humanos, como também o desenvolvimento de certas características autónomas e cognitivas – por exemplo, a capacidade de aprender com a experiência e de tomar decisões quase independentes – os tornaram cada vez mais similares a agentes que interagem com o seu ambiente e conseguem alterá-lo de forma significativa"; mas também na previsão daquilo que possivelmente acontecerá no futuro, isto é, observando o ritmo de evolução das novas tecnologias, o Parlamento Europeu não descartou a hipótese de a inteligência artificial ultrapassar a capacidade intelectual humana.

Certo é que, diante do decurso expectável da inovação na inteligência artificial, será cada vez menos utópica uma realidade onde a inteligência artificial abarcará entidades que não passarão de meros instrumentos nas mãos do seu utilizador ou proprietário, bem como entidades que gozarão de uma capacidade cognitiva e volitiva próximas das que são habitualmente associadas à espécie humana. Assim sendo, coloca-se a questão da responsabilidade civil, pois que foi essa a preocupação do Parlamento Europeu, num quadro de hipóteses onde os robôs deixam de ser meras coisas instrumentalizadas pelo fabricante, operador, proprietário ou utilizador, tomam decisões autónomas e independentes que são causadoras de danos e se procura descortinar quem deverá ser obrigado a proceder ao pagamento de uma indemnização e reparação dos danos. Nem sempre será cristalina a determinação do responsável humano pela atuação do robô quer estejamos no domínio da responsabilidade extracontratual quer no da responsabilidade contratual, pelo menos atendendo ao regime jurídico atual.

Mas a Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica é, como se depreende do seu título, limitada ao campo do direito civil, dando particular ênfase à questão da responsabilidade civil, não se podendo dizer por isso que estejamos perante

uma proposta holística sobre a regulamentação da inteligência artificial. Por outro lado, a resposta da Comissão Europeia, através do documento SP (2017) 310[4], ficou um pouco aquém do potencial legislativo contido na Resolução do Parlamento Europeu[5].

O nosso propósito com este artigo é o de forma assumidamente breve mencionar alguns dos desafios jurídicos que a produção e utilização de veículos autónomos suscitam, partindo de uma figura jurídico-penal como o direito de necessidade previsto no artigo 34.º do CP, não no sentido de considerar a sua aplicação direta e autónoma aos veículos autónomos, mas chamando à colação alguns dos problemas que a seu propósito se colocam e que, cremos, possuem relevância neste domínio.

2. DIREITO DE NECESSIDADE

No direito penal português, a figura do direito de necessidade, apelidado igualmente de estado de necessidade objetivo ou justificante, tem como efeito, quando preenchidas as suas premissas, a exclusão da ilicitude de um comportamento jurídico-penalmente relevante. Distingue-se, neste aspeto, do estado de necessidade desculpante ou subjetivo. Este último limita-se a afastar a culpa do agente. Portanto, embora as duas figuras – direito de necessidade e estado de necessidade (desculpante) – radiquem na existência de um conflito de interesses juridicamente protegidos, só na primeira delas a prática de uma conduta típica destinada a afastar um perigo atual que ameace interesses jurídicos do agente ou de terceiro não será considerada ilícita.

Um dos pressupostos de maior monta do direito de necessidade é o de que o interesse salvaguardado pela conduta típica do agente seja de valor sensivelmente superior ao sacrificado (art.º 34.º, al. b do CP). Não basta, pois, que haja superioridade de um interesse relativamente ao outro. A lei exige que da ponderação do valor dos interesses conflituantes se conclua a sensível superioridade do interesse salvaguardado,

4 Cf. http://www.europarl.europa.eu/oeil/spdoc.do?i=28110&j=0&l=en.
5 Cf. porém Daniel Schlaepfer e Hugo Kruyne, "AI and robots should not be attributed legal personhood", disponível no site https://www.euractiv.com/section/economy-jobs/opinion/ai-and-robots-should-not-be-attributed-legal-personhood/, onde se antecipa que "[b]y the end of April, the European Commission will be announcing «an initiative on Artificial Intelligence and robotics»".

sob pena de a conduta ser tida como ilícita, restando ao agente uma possível exclusão da sua culpa pelo estado de necessidade (art.º 35.º).

Para aferir-se a existência de uma sensível superioridade de um dos interesses em conflito, a doutrina jurídico-penal portuguesa e estrangeira oferece pontos de vista ou critérios ponderadores múltiplos[6].

Em primeiro lugar, as molduras penais associadas à sua violação. Na hipótese de estarmos perante um conflito de interesses jurídico-penalmente tutelados, o que nem sempre acontece, pois que, por vezes, um dos interesses conflituantes tem natureza não penal, a prevalência de um relativamente ao outro poderá sustentar-se na intensidade da moldura abstrata da pena prevista no tipo legal de crime que tutela o bem jurídico-penal. A título de exemplo, compare-se a moldura de um a oito anos de prisão prevista no artigo 131.º do Código Penal aplicável a quem pratique o crime de homicídio, com o qual se tutela o bem jurídico vida, com a moldura de um mês a três anos de prisão ou pena de multa aplicável no crime de furto consagrado no artigo 203.º do mesmo diploma legal, onde está em causa a propriedade. Comparando estas molduras abstratas, parece evidente que a vida se situa num patamar de importância superior ao da propriedade.

Um outro critério ponderador reside na intensidade da lesão do bem jurídico, isto é, terá de avaliar-se qual o grau de lesão de cada um dos bens jurídicos ou interesses, se parcial ou total, se passageiro ou permanente. Este critério é especialmente relevante quando os bens jurídicos em confronto são de importância semelhante, mas também quando um deles seria *ab initio* superior, mas, por força das circunstâncias do caso em concreto, seja lesado num *quantum* manifestamente inferior ao do outro bem jurídico, o que leva a que, para efeitos de direito de necessidade, o primeiro seja *in casu* hierarquicamente inferior. Recorrendo a um exemplo oferecido por Figueiredo Dias, os "bens jurídicos "integridade física" (art. 143.º e ss.) ou "liberdade pessoal" (art. 153.º) devem em regra, reputar-se de superior hierarquia à de bens jurídicos puramente patrimoniais (...) e todavia não haverá dúvidas que para afastamento de um grave prejuízo patrimonial (v. g., derivado de um incêndio em habitação ou casa comercial),

6 Cf. ROXIN, Claus, *Derecho Penal, Parte General, Tomo I*, Madrid, Civitas, 1997, pp. 682 e ss., bem como DIAS, Figueiredo, *Direito penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime*, Coimbra Editora, Coimbra, 2012, pp. 445 e ss.

deve ter-se por justificado o empurrão que o bombeiro dá a um "mirone" e que lhe determina uma pequena lesão corporal (art. 143.º) "[7].

O grau de perigo pode constituir um terceiro critério a tomar em consideração. Quando para a proteção de um bem jurídico definitivamente em risco, o agente assuma uma ação de salvamento que se traduza na produção de um perigo de menor importância relativa, a sua conduta deverá ser justificada à luz do direito de necessidade. Será o caso do condutor de ambulância que transporta um doente grave a necessitar de cuidados médicos urgentes e conduz a alta velocidade pondo em perigo a vida ou integridade física de quem circula na estrada.

A autonomia pessoal do lesado e o seu papel no direito de necessidade tem merecido amplo debate na doutrina. Se para uns Autores, a autonomia pessoal do lesado constitui um limite inultrapassável à ponderação de interesses conflituantes, para outros, porém, tal configuração da natureza da autonomia pessoal do lesado resulta de uma confusão entre a autonomia pessoal e a eminente dignidade da pessoa, razão pela qual escolhem imputar à autonomia pessoal, nas hipóteses de conflito em que um dos bens jurídicos é eminentemente pessoal, relevância no juízo de valoração dos interessantes conflituantes. Novamente, com Figueiredo Dias, se não está justificada, por melindrar de modo irrazoável, a "intervenção médica destinada a retirar. Sem o seu consentimento, um rim a *A*, cheio de saúde e que poderá viver certamente só com o rim restante, mesmo que essa seja a única forma de, por via de transplante, salvar a vida de B: a tanto se opõe - apesar de o bem jurídico "vida de B" ser de hierarquia superior ao da "integridade física de A" (...) Mas (...) o mesmo já não deverá defender-se para o caso de C ser forçado - sem nenhum prejuízo grave para si a dar sangue, por ser a única pessoa com o tipo necessário a uma intervenção cirúrgica urgente, indispensável à salvação da vida da vida de *D*"[8].

7 Cf. DIAS, Figueiredo, *Direito penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime*, Coimbra Editora, Coimbra, 2012, p. 447.
8 Cf. DIAS, Figueiredo, *Direito penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime*, Coimbra Editora, Coimbra, 2012, pp. 449-450.

Problema particularmente relevante coloca-se a propósito da (im)ponderabilidade da vida humana, do qual podemos nutrir ensinamentos importantes para a questão que constitui o cerne deste artigo[9].

Uma afirmação de princípio neste domínio consiste em defender que a vida humana não é ponderável em dois sentidos: quantitativo e qualitativo. No quadro de valores que se encontram consagrados constitucionalmente a justificação de uma conduta lesiva da vida humana é, em regra[10], excluída, logo porque a vida humana, pelas suas caraterísticas de incomparabilidade e impossibilidade de substituição, ocupa lugar cimeiro dos bens jurídicos. Por esse motivo se compreende que razões de ordem aritmética não constituam, para doutrina qualificada, argumento suficiente para, numa hipótese de conflito de vidas contra vida, se optar por salvar o maior número de vidas e, desse modo, beneficiar do regime do direito de necessidade. A mesma conclusão se alcançará quando haja a tentação de se tomar em consideração fatores de cariz qualitativo das vidas em conflito, por exemplo a idade, condição de saúde, etc. Em suma, pode dizer-se que "uma vida vale exactamente o mesmo que dez, cem ou mil vidas, porventura o mesmo que todo o resto da humanidade"[11].

3. VEÍCULOS AUTÓNOMOS: DEFINIÇÃO

Os veículos autónomos são capazes de circular sem *input* por parte de um condutor. A autonomia e configuração deste tipo de veículos é variável, indo desde, por exemplo, carros dotados de câmaras e sensores capazes de captar o ambiente circundante e detetar obstáculos, marcações na estrada ou sinalização, conduzindo autonomamente, mas dependentes de um condutor para retomar o comando do carro a

9 Cf. ROXIN, Claus, *Derecho Penal, Parte General, Tomo I*, Madrid, Civitas, 1997, pp. 686 e ss.
10 A dúvida instala-se, porém, nos casos denominados de comunidade de perigo. Cf. ROXIN, Claus, *Derecho Penal, Parte General, Tomo I*, Madrid, Civitas, 1997, pp. 687 e ss. De todo o modo, não podemos ignorar neste contexto que uma conduta que lese a vida de outrem pode justificar-se, se preenchidos os pressupostos legais, por força do instituto da legítima defesa ou do conflito de deveres.
11 Cf. DIAS, Figueiredo, *Direito penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime*, Coimbra Editora, Coimbra, 2012, p. 451.

qualquer momento, a carros que dispensam completamente peças tidas como básicas da condução automóvel, como o volante ou pedais.

Com a automatização dos veículos pretende-se lograr uma maior mobilidade, conforto, eficiência, produtividade, qualidade de vida, redução das emissões de gases poluentes e, sobretudo, diminuição do número de acidentes, designadamente aqueles que têm na sua origem comportamentos humanos negligentes ou imprudentes. De acordo com o Departamento de Transportes norte-americano[12], ocorreram desde 1966 mais de 2 milhões de acidentes mortais nos Estados Unidos, sendo que em 94% deles encontra-se uma falha humana. Razão pela qual se deposita nos avanços das tecnologias associadas aos transportes autónomos a esperança de um futuro em que as mortes e ferimentos – e custos associados – causados pelo recurso a transportes tradicionais sejam fortemente mitigados.

No entanto, a inovação e desenvolvimento das tecnologias de automatização têm de ser realizados de acordo com *standards* que assegurem a segurança dos transportes atuais. Isto é, embora seja de inegável nobreza o objetivo final de salvamento de vidas, não pode este ser obtido a qualquer custo, *v.g.* transformando as atuais estradas em autênticos laboratórios de experimentação, pondo em perigo quem nelas circula.

Quanto à automatização de veículos, torna-se necessário explicitar um pouco melhor este conceito, para sabermos exatamente com o que estamos a lidar. Ora, a *National Highway Traffic Safety Administration* dos Estados Unidos da América[13] adota a classificação proposta pela Society of Automotive Engineers quanto ao grau de autonomia de veículos, nos seguintes termos:

Nível 0 – As tarefas de condução são realizadas exclusivamente pelo condutor, não existindo qualquer autonomia do veículo.

Nível 1 – O veículo está equipado com algumas tecnologias de auxílio à condução, mas continua dependente do *input* do condutor.

12 Cf. prefácio da autoria da Secretária Elaine L. Chao do Departmento de Transportes, em National Highway Traffic Safety Administration, "Automated driving systems 2.0. A vision for safety", disponível em https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.
13 Cf. National Highway Traffic Safety Administration, "Automated driving systems 2.0. A vision for safety", disponível em https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

Nível 2 – Há a inclusão de funções como o controlo automático da aceleração e direção do veículo, embora o condutor não seja dispensável e tenha de permanecer envolvido na atividade de condução e atento ao meio ambiente circundante. Trata-se de uma autonomia parcial.

Nível 3 – Aqui já estamos perante uma autonomia condicional. O condutor deve estar pronto a assumir os comandos do veículo, em caso de necessidade, mas o veículo é autónomo o suficiente para não se exigir ao condutor a monitorização do ambiente circundante. Em caso de acidente iminente, o veículo é capaz de tomar decisões autónomas como desviar-se de um outro veículo que dele se aproxima ou mudar de faixa quando estejam reunidas as condições de segurança necessárias. O condutor é somente um "sistema de recurso".

Nível 4 – A autonomia de nível 4 é elevada o suficiente para que o veículo possa circular autonomamente, sem intervenção alguma do condutor, em determinadas condições, nomeadamente geoespaciais. Ao condutor é atribuída a possibilidade de tomar o controlo do veículo.

Nível 5 – Este é o último nível de autonomia. Carateriza-se por dispensar completamente a intervenção humana, em qualquer condição. Pode atribuir-se ao condutor a possibilidade de controlar o veículo, mas este é dotado de tecnologia suficientemente avançada para identificar as condições da estrada, interpretar sinais de trânsito, possíveis obstáculos, quer de dia quer de noite, reagindo dinamicamente a qualquer situação que possa ocorrer.

4.REGULAMENTAÇÃO JURÍDICA: O CASO ALEMÃO

Um dos países pioneiros na regulamentação de veículos autónomos é a Alemanha. As razões que o explicam adivinham-se facilmente. Bastará recordar a importância da indústria alemã na economia nacional daquele país.

Com a 8.ª alteração (*Achtes Gesetz zur Änderung des Straßenverkehrsgesetzes*) [14] ao Código da Estrada (*Straßenverkehrsgesetz*)[15], de 16 de junho de 2017, foram introduzidos cinco artigos (§1a, §1b, §1c, §63a e §63b) a este propósito. De forma muito sumária, os pontos-chave aí encontrados são a definição de veículos parcialmente ou totalmente autónomos; permissão da utilização de veículos autónomos desde que assegure a presença permanente de um condutor que, a qualquer momento, possa assumir o controlo do veículo; e a obrigação de os veículos serem equipados com uma caixa negra onde os dados relacionados com a condução fiquem registados e possam ser acedidos em caso de acidente.

Não pode deixar de mencionado também o trabalho da Comissão de Ética do Ministério Federal dos Transportes e Infraestruturas Digitais, apresentado em Agosto de 2017[16], do qual resultou um conjunto de orientações éticas[17] que devem nortear a programação de veículos autónomos. Pela sua importância aqui deixamos a sua enunciação[18]:

1. O principal objetivo dos sistemas de transporte parcialmente e totalmente automatizados é melhorar a segurança de todos. Outro objetivo é aumentar as oportunidades de mobilidade e possibilitar benefícios adicionais. O desenvolvimento tecnológico obedece ao princípio da autonomia pessoal, o que significa que os indivíduos gozam de liberdade de ação para a qual eles próprios são responsáveis.

2. A proteção dos indivíduos prevalece sobre todas as outras considerações utilitárias. O objetivo é reduzir o nível de dano até que seja completamente prevenido. O licenciamento de sistemas automatizados não é justificável, a menos que prometa produzir pelo menos uma diminuição de danos em comparação com a condução humana, ou seja, um saldo positivo de riscos.

3. O setor público é responsável por garantir a segurança dos sistemas automatizados e conectados introduzidos e licenciados no ambiente de rua pública. Os

14 Cf. https://www.cr-online.de/bgbl117s1648_75404.pdf.
15 Cf. https://www.gesetze-im-internet.de/stvg/BJNR004370909.html.
16 Cf. http://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2017/128-dobrindt-massnahmenplan-ethikregeln-fahrcomputer.html.
17 Cf. https://www.bmvi.de/SharedDocs/EN/Documents/G/ethic-commission-report.pdf?__blob=publicationFile.
18 Tradução realizada pelo Autor deste artigo.

sistemas de condução, portanto, precisam de licenciamento e monitoramento oficial. O princípio orientador é a prevenção de acidentes, embora os riscos residuais tecnologicamente inevitáveis não militem contra a introdução da condução automatizada se o equilíbrio de riscos for fundamentalmente positivo.

4. A responsabilidade pessoal dos indivíduos para tomar decisões é uma expressão de uma sociedade centrada em seres humanos individuais, com o seu direito ao desenvolvimento pessoal e sua necessidade de proteção. O objetivo de todas as decisões regulatórias governamentais e políticas é, assim, promover o desenvolvimento livre e a proteção dos indivíduos. Numa sociedade livre, a forma como a tecnologia é descrita estatutariamente é tal que um equilíbrio é atingido entre a máxima liberdade de escolha pessoal em um regime geral de desenvolvimento e a liberdade de outros e a sua segurança.

5. A tecnologia automatizada e conectada deve evitar acidentes sempre que isso seja praticamente possível. Com base no estado da arte, a tecnologia deve ser projetada de tal forma que situações críticas sejam evitadas. Estas incluem situações de dilema, ou seja, uma situação em que um veículo automatizado tem de "decidir" qual de dois males, entre os quais não pode haver uma solução de compromisso, ele necessariamente tem de executar. Neste contexto, todo o espectro de opções tecnológicas - por exemplo, de limitar o escopo da aplicação a ambientes de tráfego controláveis, sensores de veículos e desempenho de travagem, sinais para pessoas em risco, até à prevenção de perigos por meio de infraestruturas rodoviárias "inteligentes" - deve ser usado e evoluído continuamente. O aprimoramento significativo da segurança rodoviária é o objetivo do desenvolvimento e da regulamentação, começando pelo *design* e programação dos veículos, de modo a que circulem de forma defensiva e antecipatória, colocando o menor risco possível para pessoas vulneráveis na estrada.

6. A introdução de sistemas de condução mais automatizados, especialmente com a opção de prevenção automática de colisão, pode ser aceite social e eticamente se puder desbloquear o potencial existente de limitação de danos. Por outro lado, uma obrigação legalmente imposta de utilizar sistemas de transporte totalmente automatizados ou a sua imposição prática é eticamente questionável se implicar a submissão a imperativos tecnológicos (proibição de degradar o sujeito a um mero elemento de rede).

7. Em situações perigosas que se revelem inevitáveis, apesar de todas as precauções tecnológicas serem tomadas, a proteção da vida humana goza de máxima prioridade no equilíbrio de interesses legalmente protegidos. Assim, dentro das restrições do que é tecnologicamente viável, os sistemas devem ser programados para aceitar danos aos animais ou propriedade em um conflito, se isso significar o evitamento de danos pessoais.

8. As decisões dilemáticas genuínas, como uma decisão entre uma vida humana e outra, dependem da situação concreta, incorporando o comportamento "imprevisível" das partes afetadas. Elas não podem, portanto, ser claramente padronizados, nem podem ser programados de forma que sejam eticamente inquestionáveis. Os sistemas tecnológicos devem ser projetados para evitar acidentes. No entanto, eles não podem ser padronizados para uma avaliação complexa ou intuitiva dos impactos de um acidente de tal forma que eles possam substituir ou antecipar a decisão de um condutor responsável com a capacidade moral de fazer julgamentos corretos. É verdade que um condutor humano estaria agindo ilegalmente se ele matasse uma pessoa em uma emergência para salvar a vida de uma ou mais pessoas, mas ele não iria necessariamente agir com culpa. Tais julgamentos legais, feitos em retrospetiva e levando em consideração circunstâncias especiais, não podem ser facilmente transformados em avaliações *ex ante* genéricas ou abstratas e, consequentemente, em rotinas de programação correspondentes. Por esta razão, talvez mais do que qualquer outra, seria desejável que uma agência do setor público independente (por exemplo, uma Agência Federal para a Investigação de Acidentes envolvendo Sistemas Automatizados de Transporte ou um Departamento Federal para a Segurança em Transportes Automatizados e Conectados) processasse de forma sistemática as lições aprendidas.

9. No caso de situações de acidentes inevitáveis, qualquer distinção baseada em características pessoais (idade, género, constituição física ou mental) é estritamente proibida. Também é proibido compensar umas vítimas com outras. A programação no sentido de reduzir o número de ferimentos pessoais pode ser justificável. As partes envolvidas na geração de riscos de mobilidade não devem sacrificar as partes não envolvidas.

10. No caso de sistemas de condução conectados e automatizados, a responsabilidade que anteriormente residia no indivíduo desloca-se do condutor para os

fabricantes e operadores dos sistemas tecnológicos e para os órgãos responsáveis pela tomada de decisões políticas, legais e sobre infraestruturas. Os regimes jurídicos de responsabilidade e a sua concretização nas decisões quotidianas tomadas pelos tribunais devem refletir adequadamente esta transição.

11. A responsabilidade por danos causados por sistemas de condução automáticos ativados é regida pelos mesmos princípios que a responsabilidade por outros produtos. Assim, os fabricantes ou operadores estão obrigados a otimizar continuamente os seus sistemas e a observar os sistemas que já entregaram e aprimorá-los onde isso seja tecnologicamente possível e razoável.

12. O público tem o direito a uma informação suficientemente diferenciada sobre as novas tecnologias e seu uso. Para a implementação prática dos princípios aqui desenvolvidos, as diretrizes para o uso e programação de veículos automatizados devem ser divisadas de forma tão transparente quanto possível e comunicadas em público e revistas por um órgão independente tecnicamente adequado.

13. Não é possível afirmar hoje se, no futuro, será possível e conveniente ter a conectividade completa e o controlo central de todos os veículos a motor no contexto de uma infraestrutura de transporte digital, semelhante à dos setores de caminhos-de-ferro e de aviação. A conectividade completa e o controlo central de todos os veículos a motor no contexto de uma infraestrutura de transporte digital são eticamente questionáveis se, e na medida em que, não se seja capaz de excluir com segurança a vigilância total dos condutores e a manipulação do controlo do veículo.

14. A condução automatizada é justificável apenas na medida em que os ataques concebíveis, em particular a manipulação do sistema informático ou das fraquezas do sistema inato, não resultem em danos que possam prejudicar a confiança das pessoas no transporte rodoviário.

15. Os modelos empresariais permitidos que utilizam os dados que são gerados pela condução automática e conectada e que são relevantes ou não para o controlo do veículo enfrentam limites decorrentes da autonomia e da soberania dos dados dos condutores. São os proprietários dos veículos e os condutores que decidem se os dados do veículo que são gerados devem ser encaminhados e usados. A natureza voluntária

dessa divulgação de dados pressupõe a existência de alternativas sérias e sua exequibilidade. Devem ser tomadas medidas numa fase inicial para contrariar uma força normativa da factualidade, como a que prevalece no caso de acesso de dados pelos operadores de motores de busca ou redes sociais.

16. Deve ser possível distinguir claramente se um sistema autónomo sem condutor está a ser usado ou se um condutor com a possibilidade de retorno do controlo mantém a responsabilidade. No caso de sistemas sem condutores, a interface homem-máquina deve ser projetada para que, em qualquer momento, seja claramente regulada e aparente em que lado as responsabilidades individuais recaem, especialmente a responsabilidade pelo controlo. A distribuição das responsabilidades, por exemplo no que diz respeito ao tempo e acesso, deve ser documentada e armazenada. Isto aplica-se especialmente aos procedimentos de transferência de humano a tecnologia. A padronização internacional dos procedimentos de entrega e sua documentação (*log*) devem ser almejadas para garantir a compatibilidade das obrigações de registo ou documentação à medida que as tecnologias automobilísticas e digitais cruzam cada vez mais as fronteiras nacionais.

17. O *software* e a tecnologia de veículos altamente automatizados devem ser projetados de modo que a necessidade de uma transferência abrupta do controlo para o condutor ("estado de emergência") seja virtualmente evitada. Para permitir uma comunicação humano-máquina eficiente e segura e evitar sobrecargas excessivas, os sistemas devem adaptar-se mais ao comportamento comunicativo humano em vez de exigir que os humanos aprimorem as suas capacidades adaptativas.

18. Os sistemas de autoaprendizagem e a sua ligação a bases de dados centrais de cenários podem ser eticamente aceites se, e na medida que, gerarem ganhos de segurança. Os sistemas de autoaprendizagem não devem ser usados a menos que atendam aos requisitos de segurança relativos às funções relevantes para o controlo do veículo e não prejudiquem as regras aqui estabelecidas. Parece sensato transferir cenários relevantes para um catálogo central de cenários em uma entidade neutra, a fim de desenvolver padrões universais apropriados, incluindo quaisquer testes de aceitação.

19. Em situações de emergência, o veículo deve, de forma autónoma, sem assistência humana, entrar num "estado seguro". É desejável a harmonização, especialmente da definição de um estado seguro ou das rotinas de entrega.

20. O uso adequado de sistemas automatizados deve fazer parte da educação digital geral das pessoas. O uso adequado de sistemas automáticos de condução deve ser ensinado e testado de maneira apropriada durante as aulas de condução.

5. A PROPOSTA ALEMÃ NO CONTEXTO DE INTERESSES CONFLITUANTES

Há algumas ideias interessantes a retirar do conjunto de orientações acima enunciadas quando confrontadas com a questão de conflitos de interesses. Em primeiro lugar, deverá ser estabelecida uma hierarquia dos interesses conflituantes encabeçada pela proteção da vida humana. Por isso, num cenário em que o veículo haja de decidir entre a lesão da vida humana ou danos contra a propriedade ou animais, o primeiro dos interesses merecerá prioridade. A subordinação de interesses patrimoniais também se mantém quando do outro lado esteja em causa a possibilidade de lesões pessoais.

Estes critérios de ponderação, encontrados no ponto 7, merecem-nos algumas dúvidas. De acordo com o que ficou expendido a propósito do direito de necessidade jurídico-penal é no mínimo discutível que se cristalize uma solução definitiva e apriorística atendendo unicamente aos interesses conflituantes perspetivados abstratamente e sem sopesar os diversos elementos compositivos da situação global concreta onde se suscita a opção por um desses interesses. Mesmo que um dos interesses conflituantes seja a integridade física de um transeunte, por exemplo, e o outro a proteção de uma estátua de grande valor artístico, a determinação da hierarquia concreta entre estes dois interesses nem por isso é facilitada. Imagine-se que para evitar um dano considerável na dita estátua se faz necessário produzir uma ofensa à integridade física leve de um transeunte. Se aplicarmos cegamente o critério proposto, a integridade física deveria sobrepor-se ao património, quando sabemos que a intensidade da lesão do primeiro interesse é largamente superior ao do segundo, a ponto de, no âmbito do direito penal, perante este dilema, se justificar a conduta de quem sacrifique a integridade física. Ademais, ainda que um dos interesses conflituantes fosse a vida humana, poderia acontecer que no outro lado da balança se encontrasse a lesão da autonomia pessoal de

outrem, o que levaria, em certas hipóteses, à tutela desta última em detrimento da primeira.

Podemos também afirmar sem mais que o património deve situar-se no mesmo patamar de importância que a vida de um animal? No ordenamento jurídico português, com a entrada em vigor da Lei n.º 8/2007, de 3 de março, consagrou-se o estatuto jurídico dos animais, com o qual se reconheceu aos animais a natureza de seres vivos dotados de sensibilidade. Esta distinção ontológica e jurídica entre património e animais é encontrada também em outros ordenamentos jurídicos, não aparecendo como um sinal idiossincrático português. É no mínimo estranho que, numa lógica puramente abstrata, se coloque a vida e integridade humana acima de animais e património, mas não se hierarquizem estes últimos dois, como se realidades idênticas se tratassem.

Por estas razões, reiteramos, é duvidosa a solução proposta no sentido de programar os referidos sistemas autónomos para salvaguardarem a vida e integridade físicas e sacrificarem os demais interesses.

Já o exposto no ponto 9 não nos merece repúdio absoluto. Deixámos exposta a nossa posição quando alertamos para, em caso de conflito de vida contra vida, considerações de tipo quantitativo ou qualitativo, *v.g.* idade, género, constituição física ou mental não poderem amontar a critérios ponderadores.

A merecer maior questionamento é a proposta principiológica de diminuição de ferimentos pessoais enquanto linha orientadora da programação de veículos autónomos. Compreende-se medianamente que se programe um veículo para em situações de colisões inevitáveis, por exemplo, procurar causar o menor dano possível. Mas são colocados de parte pontos de vista como o da intensidade da lesão do bem jurídico, o grau de perigo ou mesmo o da autonomia pessoal.

E se estivermos perante conflito de vidas? Imagine-se que *A*, condutor de um veículo autónomo de nível 5, é surpreendido pela queda de uma árvore na estrada onde circula e existe apenas o tempo suficiente para o veículo tomar uma decisão: mantém-se na estrada, provocando o embate na árvore e a morte do condutor ou galga o passeio e atropela mortalmente duas pessoas. O que deve o automóvel fazer? Estivesse o condutor em controlo do veículo e tivesse a oportunidade de tomar uma opção, a decisão

deste conflito existencial radicaria numa atitude íntima de abnegação (ou não) da sua própria vida. Não sendo possível colocar nas mãos do condutor esta decisão, em que medida e com que legitimidade pode o produtor ou programador do veículo autónomo antecipar um conflito como o descrito e impor uma solução genérica de uma complexidade ética abissal? E se estivermos perante veículos com um elevadíssimo grau de autonomia e capacidade de decisão e aprendizagem que o tornem capaz de traçar, *in illo tempore*, o destino de uma ou mais vidas humanas? A solução seria distinta num cenário em que as vidas de todos os intervenientes estavam definitivamente condenadas e ao veículo incumbisse "somente" salvar o maior número de pessoas possível?

São mais as interrogações que se colocam que eventuais caminhos de solução. O momento de as colocar é, no entanto, agora, no início da revolução da inteligência artificial, quando ainda é útil e eficaz gizar os traços norteadores do seu desenvolvimento.

6. CONSIDERAÇÕES FINAIS

Em jeito de conclusão, diremos que os veículos autónomos, em especial os de nível 5, contêm a génese de uma transformação radical do setor dos transportes e, mediatamente, da economia, qualidade de vida e segurança na mobilidade. No entanto, a imprevisibilidade dos contextos reais em que esses veículos irão circular demandam, desde logo, o respeito por princípios habitualmente aquilatados noutras searas jurídicas como o princípio da prevenção e o da precaução.

A tecnologia não deve ser um fim em si mesmo. Esta ideia é por demais evidente quando a sua implementação possa pôr em crise interesses especialmente significativos para a comunidade e seus membros. Urge pois pensar até onde deverá ir a inteligência artificial.

Estaremos, pois, preparados para conviver com entidades inteligentes aptas a nos transverter, metafórica e literalmente, em simples passageiros observadores diante de escolhas e decisões que nos afetam direta ou indiretamente? Quereremos, se os avanços tecnológicos assim o possibilitarem, entregar a agentes desprovidos de vida no sentido biológico do termo a assunção da responsabilidade da dissolução intuitiva, se não padronizada, de dilemas éticos?

BIBLIOGRAFIA

- DIAS, Figueiredo, Direito penal, Parte Geral, Tomo I, Questões fundamentais, A doutrina geral do crime, Coimbra Editora, Coimbra, 2012.

- FREITAS, Pedro Miguel, ANDRADE, Francisco e NOVAIS, Paulo, "Criminal Liability of Autonomous Agents: from the unthinkable to the plausible", in Pompeu Casanovas et al (Eds.), AICOL IV/V 2013, LNAI 8929, Springer, 2014, pp. 145-156.

- NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, "Automated driving systems 2.0. A vision for safety", Disponível em https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

- ROXIN, Claus, *Derecho Penal, Parte General, Tomo I*, Madrid, Civitas, 1997.

- SCHLAEPFER, Daniel e KRUYNE, Hugo, "AI and robots should not be attributed legal personhood", Disponível no site https://www.euractiv.com/section/economy-jobs/opinion/ai-and-robots-should-not-be-attributed-legal-personhood/.

CRIPTOCONTRATAÇÃO: UMA NOVA FORMA DE CONTRATAÇÃO AUTOMATIZADA?*

DANIEL DE SENNA FERNANDES [1]

* Este trabalho é uma versão abreviada da Dissertação de Mestrado da autoria de Daniel Augusto de Senna Fernandes Batalha, apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), sob orientação do Doutor Alexandre Libório Dias Pereira.

1 Correio electrónico: dannsefer@gmail.com

RESUMO

Esta investigação almeja analisar as tecnologias que apoiam as *distributed ledger technologies* (v.g. criptografia, *smart contracts* e agentes de *software*), à guisa de demonstrar que a criptocontratação se trata de uma nova forma de contratação electrónica automatizada, passando por uma tentativa de qualificação jurídica dos agentes de *software*, fundamentais nesta forma de contratação.

Dada a novidade das tecnologias envolvidas, este trabalho envolveu o estudo de artigos técnicos relacionados com as mesmas e a análise de instrumentos bibliográficos e instrumentos legais relativos à área do direito civil, concretamente sobre o negócio jurídico e a contratação electrónica.

Por fim, faremos uma incursão e reflexão sobre a questão de saber se o actual regime aplicável à contratação sem intervenção humana, previsto no artigo 33.º do Decreto-lei n.º 7/2004, de 7 de Janeiro, pode contemplar a criptocontratação (e, em caso afirmativo, se é suficiente para resolver os problemas que possam surgir em caso de conflito) ou se se deve conceber, *de jure constituendo*, um regime próprio, especificamente para a criptocontratação.

Palavras-Chave: agentes de *software*; *blockchain*; contratação automatizada; direito da informática; *distributed ledger technologies*; *smart contracts.*

1. INTRODUÇÃO

Nunca o desenvolvimento tecnológico nas áreas da robótica e da inteligência artificial sentiu um progresso tão acentuado quanto aquele que é sentido hodiernamente. Perante a rápida evolução destas áreas, é apenas natural que se formem sentimentos de curiosidade, incerteza, desconfiança e até medo do desconhecido na sociedade.

Por ocasião da 9.ª edição da Conferência *Web Summit* (uma conferência centrada na tecnologia da *internet*, que decorreu entre os dias 6 e 9 de Novembro de 2017), e que contou com a apresentação do robô Sophia, de um serviço de deslocações partilhadas pelo ar e ainda com a exposição e discussão de diversas criptomoedas, como a *Bitcoin* e a *Ethereum*, e das chamadas *Distributed Ledger Technologies* (e suas respectivas aplicações), divulgaram-se nos meios de comunicação social duas notícias com manchetes patentemente contraditórias, espaçadas por pouquíssimos dias: lia-se no dia 7 de Novembro de 2017, na manchete de uma notícia do CNBC «*Bitcoin has no future because of its anonymity, SocGen CEO says*»[1] («A *Bitcoin* não tem futuro devido ao seu intrínseco anonimato, diz presidente executivo da SocGen», numa tradução livre); poucos dias depois, a 11 de Novembro de 2017, surge outra manchete novamente sobre a *Bitcoin*, mas desta vez do RT, onde se podia ler «*Bitcoin is 'the greatest technology since the internet' – cryptocurrenty investor Tim Draper*»[2] («A *Bitcoin* é a 'melhor tecnologia desde a *internet'* – investidor em criptomoeda, Tim Draper», numa tradução livre).

Com estes dois artigos noticiosos retratando duas opiniões incontestavelmente díspares, podemos afirmar que se trata de um reflexo de sentimentos de curiosidade, incerteza, desconfiança e medo do desconhecido. É precisamente a partir desta incerteza e curiosidade que nasce o trabalho que nos propomos desenvolver; um trabalho que, por

1 Cf. R. BROWNE (2017). "Bitcoin is 'definitely not a fraud,' CEO of mobile-only bank Revolut says". *CNBC*. Obtido em 30 de Janeiro de 2018, disponível em https://www.cnbc.com/2017/11/24/revolut-signs-up-1-million-users-ahead-bitcoin-cryptocurrency-launch.html

2 Cf. RT (2017). "Bitcoin is 'the greatest technology since the internet' – cryptocurrency investor Tim Draper". *RT*. Obtido em 30 de Janeiro de 2018, disponível em https://on.rt.com/8s01

força da sua novidade, carece de apoio jurisprudencial, mas nem por isso desmerece a nossa atenção e dedicação.

Pelo exposto, esta investigação almeja analisar as tecnologias que apoiam as *distributed ledger technologies* (como o *blockchain* e o *tangle*), para que se possa determinar se a contratação automatizada com recurso a agentes de *software* se trata de uma nova forma automatizada de contratar e se o actual regime aplicável à contratação sem intervenção humana, previsto no artigo 33.º da Lei do Comércio Electrónico (Decreto-lei n.º 7/2004, de 7 de Janeiro, com as alterações dadas pelo DL n.º 62/2009, de 10 de Março, e pela Lei n.º 46/2012, de 29 de Agosto)[3] é suficiente para resolver os problemas que possam surgir em caso de conflito. Revela-se uma questão pertinente pois, se não o for, tal significa que se reclama um novo regime jurídico, adequado às características desta forma de contratar ou, no limite, uma reforma no actual regime, de maneira a adaptá-lo à realidade que se convoca.

Contudo, por constrições de espaço, não será possível fazer uma análise mais detalhada sobre as *distributed ledger technologies*, a criptografia e as modalidades da assinatura electrónica, propondo ao nosso leitor a apreciação da nossa dissertação de Mestrado, também intitulada 'Criptocontratação: uma nova forma de contratação electrónica?', disponível no repositório da Universidade de Coimbra e que veio inspirar este artigo.

Debruçar-nos-emos sobre a origem e o conceito de *smart contracts* e ainda da noção e tipologias de agentes de *software*, que constituem, a bem dizer, o cerne deste trabalho, por forma a compreender se nos deparamos, ou não, sobre uma nova forma de contratar. Para tal, procederemos a um confronto entre a contratação automatizada com recurso à transferência electrónica de dados e a contratação automatizada com recurso aos agentes de *software*, procurando demonstrar a existência de uma nova forma de contratar 'automatizadamente' que convoca a participação de agentes de *software* e recorre à criptografia para concluir negócios jurídicos sem intervenção humana. Por

3 Doravante 'LCE'.

outras palavras, apresentaremos a chamada 'criptocontratação' (do inglês *cryptocontracting*)[4].

Após um estudo mais aprofundado das características dos agentes de *software* (que, como veremos, se trata de um programa de computador destinado a actuar autonomamente 'em nome' do seu sujeito utilizador, podendo este ser dotado de capacidades de observação, padrões de comportamento e autoaprendizagem), focar-nos-emos na tentativa de qualificação jurídica e na apresentação de um eventual regime jurídico aplicável a estes. Em síntese, se o agente se trata de um mero instrumento do seu sujeito utilizador, se o agente se trata antes de um núncio, ou, ainda, se o agente de *software* poderá ser enquadrado no regime da representação.

2. AS *DISTRIBUTED LEDGER TECHNOLOGIES*

A *distributed ledger technology*, ou DLT, é uma tecnologia que recorre ao uso extensivo de criptografia para guardar, proteger e validar transacções electrónicas[5], registando-as numa base de dados electrónica cuja manutenção cabe a uma rede distribuída (ou partilhada) de participantes (chamados nodos[6]), e não mais por uma entidade centralizada, dispensando a necessidade de um sistema central de validação. Apresenta-se, destarte, como um 'sistema de livro-razão' descentralizado, aberto e público, assemelhando-se a uma base de dados, sendo a sua validação feita pelos seus utilizadores de forma local, segundo um determinado protocolo de consenso (v.g. PoW, PoS, PoC e DAG[7]). É precisamente devido a esta característica descentralização e

4 Cf. M. ROUSE (2016). *Definition: Smart Contract.* Obtido em 30 de Janeiro de 2018, disponível em http://searchcompliance.techtarget.com/definition/smart-contract.
5 Cf. ESMA (2016). *Discussion paper: Distributed Ledger Technology applied to securities markets.* Obtido em 19 de Março de 2017, disponível em https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf.
6 Um nodo (do Latim *nodus*) é um ponto de conexão ou redistribuição ou terminal de comunicação. Neste contexto, referimo-nos a 'nodo' de referência física, ou seja, um dispositivo electrónico activo ligado a uma rede e capaz de enviar, receber ou transmitir informações através de um canal de comunicação. Cf. http://www.webcitation.org/5kx5kPIKV (Obtido em 10 de Novembro de 2017).
7 Sobre o conceito de PoW, cf., nomeadamente, C. DWORK & N. MONI (1993) Pricing via Processing or Combatting Junk Mail. Obtido em 27 de Dezembro de 2017, disponível em http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.ps;
Sobre o PoW, cf. A. BACK (2002) Hashcash - A Denial of Service Counter-Measure. *Hashcash.* Obtido em 10 de Novembro de 2017, disponível em http://www.hashcash.org/papers/hashcash.pdf;

capacidade de guardar e confirmar a validade da informação em tempo real a um custo muito reduzido, que se tem em conta o potencial revolucionário no modo de funcionamento da indústria de serviços financeiros com recurso à DLT. De facto, no entender de TAPSCOTT & TAPSCOTT, estamos a aproximarmo-nos de uma mudança de paradigma: de uma *Internet of Information* para uma *Internet of Value*[8].

Podemos identificar o *Blockchain* e o *Tangle* como dois exemplos de DLT, que se distinguem, essencialmente, no sistema de consenso adoptado: no *Blockchain* recorre-se a PoW, PoS ou PoC para criar uma 'corrente' de registos, no *Tangle* recorre-se a DAG para criar uma espécie de 'trança' de registos irreversível. Porém, dada a novidade do *Tangle*[9], concentrar-nos-emos somente no *Blockchain*, que foi apresentado como a trave-mestra da criptomoeda *Bitcoin*[10].

O *Blockchain* pode ser definido como uma rede *peer-to-peer* (doravante 'p2p') que recorre a um esquema de consenso baseado em PoW, PoS ou PoC para registar e validar transacções (esquemas que se contrapõem ao esquema de funcionamento baseado na confiança, utilizado, v.g. por bancos, que recorrem a terceiros de confiança que asseguram a validade da transacção)[11]. Ou seja: a rede aplica um selo temporal a

---

Sobre o PoS, cf., designadamente, P. VASIN (2014). BlackCoin's Proof-of-Stake Protocol v2. Obtido em 27 de Dezembro de 2017, disponível em http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf; S. KING & S. NADAL (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Obtido em 27 de Dezembro de 2017, disponível em https://peercoin.net/assets/paper/peercoin-paper.pdf; V. BUTERIN (2013). Bicoin Magazine. Obtido em 27 de Dezembro de 2017, disponível em https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/;

Para uma comparação entre PoW e PoS, cf., por exemplo, BITFURY GROUP (2015). Proof of Stake versus Proof of Work. Obtido em 27 de Dezembro de 2017, disponível em http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf;

Sobre o PoC, cf., entre outros, N. GALESI, G. ATENIESE, A. FAONIO, & I. BONACINA (2014). 'Proofs of Space: When Space Is of the Essence'. *Security and Cryptography for Networks.* pp. 538-557. Obtido em 27 de Dezembro de 2017, disponível em https://sapienza.pure.elsevier.com/en/publications/proofs-of-space-when-space-is-of-the-essence-7, S. DZIEMBOWSKI, S. FAUST, V. KOLMOGOROV, & K. PIETRZAK (2013). Proofs of Space. Obtido em 27 de Dezembro de 2017, disponível em https://eprint.iacr.org/2013/796.pdf;

Sobre o DAG, cf. BTCmanager.com (2017). Obtido em 27 de Dezembro de 2017, disponível em https://btcmanager.com/dag-vs-blockchain/; THULASIRAMAN, K. & M. SWAMY (2011). *Graphs: Theory and Algorithms*. § 5.7 Acyclic Directed Graphs. pp. 118-119, J. BANG-JENSEN & G. GUTIN (2009). *Digraphs: Theory, Algorithms and Applications*. § 2.1 Acyclic Digraphs. pp. 32-34, entre outros.

8 Cf. D. TAPSCOTT & A. TAPSCOTT (2016). *Blockchain Revolution*, p. 6.

9 Cf. BTCMANAGER.COM, *op. cit., loc. cit.*, LIMO (2017). The Tangler. Obtido em 27 de Dezembro de 2017, disponível em https://www.tangleblog.com/2017/01/25/the-tech-behind-iota-explained/#comment-4719, J. BUNTINX (2016). Obtido em 27 de Dezembro de 2017, disponível em http://bitcoinist.com/iota-internet-things-without-blockchain, M. VIZARD (2017). Augmate Announces Blockchain for IOT. Obtido em 27 de Dezembro de 2017, disponível em http://www.futuriom.com/articles/news/augmate-announces-blockchain-for-iot/2017/11.

10 V. *infra*.

11 Cf. S. NAKAMOTO (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. p. 3. Obtido em 3 de Novembro de 2017, disponível em http://bitcoin.org/bitcoin.pdf; A. BACK (2002). Hashcash. *Hashcash - A Denial of Service Counter-Measure.* Obtido em 10 de Novembro de 2017, disponível em

todas as transacções (que foram assinadas electronicamente) e insere-as numa 'corrente', por via de funções *hash*[12], criando assim um registo que não pode, em regra, ser alterado sem que se crie uma nova 'cadeia'[13–14]. Destarte, quanto mais longa for a 'corrente', mais evidente será a demonstração/prova da sequência de transacções feitas entre os nodos naquele *blockchain*. É justamente este protocolo de consenso de Nakamoto – a aceitação por parte de todos os nodos do *blockchain* dos *factos* inseridos na 'cadeia' – que garante a validade destas transacções[15].

Compreende-se da exposição feita que é possível atender às (naturais) preocupações no que à privacidade dos particulares e das suas transações diz respeito, perante a reconhecida descentralização e transparência do *blockchain*. Todavia, tratando-se de *código*, é possível optar por um sistema de acesso-restrito (ou acesso-limitado)[16].

Por fim, deve fazer-se especial referência à mais recente Lei-Modelo da Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL) no âmbito da contratação electrónica: a Lei-modelo sobre registos electrónicos transmissíveis, numa tradução livre (doravante 'Lei-Modelo')[17], aplicável às DLT, sendo propósito daquela

---

http://www.hashcash.org/papers/hashcash.pdf; M. JAKOBSSON (1999). Hashcash. *Proofs of Work and Bread Pudding Protocols (extended abstract).* pp. 20-21. Obtido em 11 de Novembro de 2017, disponível em http://www.hashcash.org/papers/bread-pudding.pdf.

12 Na verdade, o *bitcoin* recorre ao uso do SHA-256 (ou SHA-2). SHA trata-se de uma *hash function* criptográfica que permite a encriptação de determinada mensagem, transformando-a num *message digest* de 32 *bytes* (equivalente a 256 *bits*). Sendo um sucessor do SHA-1, é uma das funções *hash* disponíveis mais seguras. Sobre SHA, cf., por exemplo, FIPS PUB 180-4 (2015).

13 Para que se pudesse alterar o registo, seria necessário que mais de metade dos nodos da rede (*rectius* da capacidade computacional da rede) se organizasse para, de modo concertado e simultâneo, modificar a informação constante nos seus livros-razão, forçando assim a actualização dos livros-razão dos restantes nodos para a 'nova' informação. Esta operação designa-se *fork* (cf. https://www.etymonline.com/word/fork, obtido em 10 de Março de 2018).

14 Cf. Etherzero: https://etherzero.org (obtido em 10 de Março de 2018); Etherchain: https://www.etherchain.org/hardForks (obtido em 10 de Março de 2018).

15 Cf. S. NAKAMOTO, *op. cit.*, pp. 1, 6 e 8.

16 Neste sentido, cf. P. BOUCHER (2017). *How blockchain technology could change our lives: In-depth Analysis*. p. 19. Obtido em 11 de Maio de 2017, disponível em http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf, que se refere a «*private encrypted blockchain systems*». Sobre o tema, cf., entre outros, ANTHONYLEWIS2015 (2016). 'So you want to use a blockchain for that?'. Obtido em 1 de Janeiro de 2018, disponível em https://bitsonblocks.net/2016/07/19/so-you-want-to-use-a-blockchain-for-that; V. BUTERIN, (2015b). On Public and Private Blockchains. Obtido em 1 de Janeiro de 2018, disponível em https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

17 Disponível em http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2017model.html (Obtido em 10 de Novembro de 2017).

Lei-Modelo viabilizar o uso legal de registos electrónicos transmissíveis, no mercado interno e transfronteiriço.

Das notas explicativas da Lei-Modelo revelam-se os benefícios e utilidades desta tecnologia e da importância da criação de um regime jurídico próprio que regule o comércio electrónico fundado neste tipo de tecnologias, dando particular relevo ao princípio da não discriminação do recurso aos meios de contratação electrónica e à sua equivalência funcional, fundando-se num texto tecnologicamente neutro.

3.A ASSINATURA ELECTRÓNICA

Em Portugal, foi o DL n.º 290-D/99, de 2 de Agosto, que veio regular as relações jurídicas por meios electrónicos (tendo sido posteriormente alterado pelo DL n.º 62/2003, de 3 de Abril, em resultado da transposição da Directiva 1993/93/CE[18], e, mais recentemente, pelo DL n.º 88/2009, de 9 de Abril) e que veio apresentar o conceito de assinatura electrónica[19] (na alínea b) do seu artigo 2.º): «o resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico». O legislador português, ao adoptar esta definição, distanciou-se do disposto pelo legislador comunitário[20], afastando-a de todos os meios de autenticação que não se considerassem pessoais e exclusivos[21].

18 A Directiva 1999/93/CE, que procurou desenvolver a prestação transfronteiras de serviços de certificação e trocas comerciais no âmbito do espaço económico europeu (cf. M. CAMMARATA & E. MACCARONE (2001). *Interlex: Diritto Tecnologia Informazione*. Obtido em 7 de Novembro de 2017, disponível em http://www.interlex.it/docdigit/recep1.htm), foi revogada pelo RUE 910/2014.

19 Sobre o conceito de assinatura 'tradicional', cf., designadamente, F. CARMO (2013). *Dicionário Jurídico – Contratos e Obrigações*. Vol. I, p. 24; P. NUNES (1999). *Dicionário de Tecnologia Jurídica*. 13ª Edição, p. 120; J. FRANCO & A. MARTINS (1993). *Dicionário de Conceitos e Princípios Jurídicos*. 3ª Edição, p. 102; B. GARNER (1999). *Black's Law Dictionary*. 7th Edition, p. 1387; E. JOWITT (1959). *The Dictionary of English Law*. Vol. 2, p. 1641; M. CORREIA (2009). 'Assinatura electrónica e certificação digital – Novas tendências'. *Direito da Sociedade da Informação*. Vol. VIII, p. 160.

20 Cf. n.º 1 do artigo 2.º da Directiva 1999/93/CE e n.º 10 do artigo 3.º do Regulamento (UE) 910/2014 (doravante 'eIDAS').

21 Neste sentido, cf. A. PATRÃO (2012). 'Assinaturas Electrónicas e Garantias Reais – Da viabilidade de constituição de garantias imobiliárias por meios electrónicos à luz da lei portuguesa'. *Revista do CEDOUA*, 29, p. 51.

Considerando que nos encontramos no domínio digital, no que respeita às funções essenciais da assinatura, compreende-se que o conceito de assinatura electrónica assuma um significado funcional, sendo igualmente natural que se entenda que a um documento electrónico deva ser aposto uma assinatura electrónica[22], por se tratar do sinal tecnologicamente mais próximo. É justamente neste contexto que urge distinguir as 'peças' que integram a assinatura electrónica: (i) a assinatura, que consiste no símbolo ou marca aposto no ou ao documento electrónico pelo subscritor, (ii) o acto de assinar, que se traduz no recurso a *software* para o processamento de dados do qual resulta uma assinatura electrónica, (iii) os dados de criação de assinatura[23] e (iv) o documento electrónico[24], que estabelece o nexo de ligação entre os dados de criação de assinatura e o subscritor, possibilitando ao destinatário a faculdade de verificar a autoria do documento.

O RJDEAD identifica três tipos de assinaturas electrónicas: a assinatura electrónica avançada, a assinatura digital e a assinatura electrónica qualificada[25]. Atendendo às definições plasmadas nas alíneas c), d) e g) do artigo 2.º do RJDEAD, podemos concluir que a assinatura electrónica qualificada é a assinatura mais segura, por se tratar de uma assinatura digital – que é uma modalidade de assinatura electrónica avançada[26] –, baseada num sistema criptográfico assimétrico de chave pública[27] e num certificado qualificado e concebido por via de um dispositivo seguro de criação de assinatura.

Por conseguinte, esta 'graduação' de segurança de assinaturas electrónicas resulta em diferentes efeitos jurídicos: quando o conteúdo de determinado documento electrónico for susceptível de ser representado como declaração escrita, este satisfará o requisito legal de forma escrita [28] e a força probatória do documento electrónico será distinta conforme seja aposta (i) uma assinatura electrónica simples, avançada ou digital, ou (ii) uma assinatura electrónica qualificada: (i) nos primeiros, os documentos

22 Neste sentido, cf. M. CORREIA, *op. cit.*, p. 161.
23 Cf. alínea g) do artigo 2.º do RJDEAD.
24 Cf. alínea a) do artigo 2.º do RJDEAD.
25 Cf. alíneas c), d) e g) do artigo 2.º do RJDEAD, respectivamente.
26 A assinatura electrónica avançada deve ser apta para identificar univocamente o titular como autor do documento, dependendo a sua aposição da vontade do titular (sendo criada por meios que este pode manter sob seu controlo) e, a partir da sua conexão com o documento, ser capaz de garantir a inalterabilidade do conteúdo do documento.
27 Cf. alínea d) do artigo 2.º do RJDEAD.
28 Cf. n.º 1 do artigo 3.º do RJDEAD.

electrónicos serão apreciados nos termos gerais do direito[29], (ii) nos últimos, passam a funcionar as presunções de autoria, vontade e inalterabilidade previstas nas alíneas a) a c) do n.º 1 do artigo 7.º do RJDEAD. Diversos autores[30] e alguma jurisprudência[31] identificam estas presunções como funções caracterizadoras desta modalidade de assinaturas electrónicas, especificamente: função identificadora (estabelece a autoria do documento electrónico), função de completude ou finalizadora (manifesta a conclusão do documento electrónico bem como o assentimento e/ou conhecimento do subscritor quanto às declarações e conteúdo daquele, assumindo-as como suas) e função de garantia de inalterabilidade (comprova que o documento electrónico não foi alterado desde a aposição da assinatura electrónica até à sua recepção pelo destinatário).

Posto isto, retira-se do disposto no n.º 1 do artigo 376.º do Código Civil[32] (aplicável *ex vi* n.º 2 do artigo 3.º do RJDEAD), que o documento electrónico poderá gozar de força probatória plena, desde que seja aposto a este uma assinatura electrónica qualificada, exarada ao abrigo de um certificado emitido por uma entidade certificadora que se ache credenciada. De modo inverso, o documento electrónico que não cumpra estes requisitos será apreciado segundo o livre critério do julgador.

Pelo exposto, rapidamente se chega à conclusão que a assinatura electrónica qualificada recorre, não apenas à criptografia assimétrica de chave pública para que se cumpram as suas aludidas funções[33], mas também a certificados qualificados emitidos por uma entidade certificadora[34]. É precisamente este certificado, que contém os dados do detentor do par de chaves e a sua chave pública, que irá permitir verificar a autenticidade da assinatura electrónica. Como tal, é possível equiparar o certificado a uma espécie de documento identificativo do titular de um dispositivo de criação de assinatura electrónica, pois, se tradicionalmente se verificava a autenticidade de uma

29 Cf. n.º 5 do artigo 3.º do RJDEAD.
30 Neste sentido cf., entre outros, M. CORREIA, *op. cit.*, pp. 164-165 e pp. 170-171; L. F. P. SOUSA (2016). *O Valor Probatório do Documento Eletrónico no Processo Civil*, pp. 70-71; M. T. SOUSA (2008). 'A transmissão de actos escritos das partes por meios electrónicos em processo civil'. *APTS: Alves Pereira & Teixeira de Sousa, RL.*, pp. 29-33. Obtido em 8 de Novembro de 2017, disponível em http://www.alvespereira.com/wp-content/uploads/a-transmissao-de-actos-escritos-das-partes-por-meios-electronicos-em-processo-civil.pdf; M. ROCHA, M. CORREIA, M. RODRIGUES, M. ANDRADE & H. CARREIRO (2000). *As Leis do Comércio Electrónico*, pp. 72-74; J. PEREIRA (2004). *Compêndio Jurídico da Sociedade da Informação*, p. 203.
31 Cf., designadamente, Ac. STA de 12-03-2015, Ac. STA de 20-06-2012, Ac. TCA Sul de 15-01-2015 (Processo 11671/14), Ac. TCA Sul de 19-05-2016 (Processo 13093/16), todos disponíveis em www.dgsi.pt.
32 Doravante 'CC'.
33 Cf. M. CORREIA, *op. cit.*, p. 162.
34 Cf. alíneas g), o) a q) do artigo 2.º e artigos 24.º e 29.º, todos do RJDEAD.

assinatura autógrafa comparando-a a um documento de identificação do subscritor, neste contexto, é a assinatura electrónica verificada (pelo destinatário ou por um terceiro que pretenda fiscalizar a autoria da assinatura) pelo referido certificado[35].

Verificada a autenticidade da assinatura, dá-se por lançada a primeira pedra para o desenvolvimento da contratação electrónica: na verdade, o n.º 1 do artigo 6.º do RJDEAD refere-se à transmissão de documentos electrónicos por um meio de telecomunicações para determinado endereço electrónico que deverá ser convencionado, expressa ou tacitamente. Assim, poderá ser expressamente convencionado o endereço electrónico das partes, v.g. num acordo de transferência electrónica de dados[36].

Além disso, no que respeita à transferência electrónica de documentos electrónicos, o legislador pátrio definiu, na alínea u) do artigo 2.º do RJDEAD, a validação cronológica como «a declaração [...] que atesta a data e hora da criação, expedição ou recepção de um documento electrónico», sendo estes dados oponíveis entre as partes, e a terceiros, quando esta validação seja emitida por entidade certificadora. Se o documento electrónico contiver uma assinatura electrónica qualificada, a sua expedição poderá ser equiparada à carta registada, quando seja feita por via de telecomunicação que assegure a sua efectiva recepção. Por outro lado, se à recepção corresponder o envio de uma mensagem de confirmação subscrita com assinatura electrónica qualificada e dirigida ao remetente, equivalerá à carta registada com aviso de recepção[37]. Referindo-se a este mesmo conceito, o legislador comunitário optou por denominar este conceito de «selo temporal» ou «*time stamping*», estando esta figura definida e regulada nos n.º 33 e 34 do artigo 3.º e nos artigos 41.º e seguintes, do eIDAS.

35 Cf. M. CORREIA *op. cit.*, p. 175 e M. ROCHA (2002). 'A assinatura electrónica: Uma Via Portuguesa "Original"?'. *ASF*, p. 2. Obtido em 8 de Novembro de 2017, disponível em http://www.asf.com.pt/winlib/cgi/winlibimg.exe?key=&doc=10038&img=961.
36 Cf. artigo 1.1 da Recomendação da Comissão 94/820/CE, de 19 de Outubro, relativa aos aspectos jurídicos da transferência electrónica de dados – doravante 'atEDI'.
37 Cf. n.º 2 e 3 do artigo 6.º do RJDEAD.

4. *SMART CONTRACTS* E AGENTES DE *SOFTWARE*

4.1-Origem e noção de *smart contracts*

A *bitcoin* trata-se de uma criptomoeda criada por Satoshi Nakamoto[38] que assenta num sistema p2p, cujas transacções são verificadas por nodos e registadas numa base de dados distribuída, sem recurso a um repositório central (ou administrador único)[39]. É precisamente no artigo técnico[40] em que é divulgada esta criptomoeda que encontramos o aludido *blockchain*, que inspirou outros programadores no desenvolvimento de novas aplicações desta tecnologia.

Há autores que consideram o *Bitcoin* de *per si* menos relevante, por se tratar apenas de 'dinheiro'; são antes as inúmeras aplicações da tecnologia *blockchain* que merecem a sua (e a nossa) total atenção[41]. É neste contexto que se manifesta a chamada Crypto 2.0[42] (ou Criptografia 2.0), que se traduz, como já se adivinha, na implementação do *blockchain* (ou outro DLT) em ambientes diversos, para além de um sistema de pagamentos digital.

É justamente a limitação da *Bitcoin*, enquanto plataforma digital de pagamentos, que inspira a criação de novas plataformas, como o Ethereum[43] e o NXT[44]: tratando-se de plataformas descentralizadas, baseadas no *blockchain* de NAKAMOTO, estão aptas para, não apenas permitir aos seus utilizadores a realização de pagamentos sem recurso a terceiros, mas também executar *smart contracts* mais complexos. Por outras palavras, o acervo digital do *blockchain* daquelas plataformas poderia passar a representar, além

38 Cf. J. DAVIS (2011). 'The Crypto-Currency: Bitcoin and its mysterious inventor'. *The New Yorker*. Obtido em 10 de Março de 2017, disponível em https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.
39 Sobre as principais características da *bitcoin*, cf., entre outros, A. SAVELYEV (2017). 'Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law.' *Journal Information & Communications Technology Law* 26 (2), pp. 116-134. Obtido em 14 de Novembro de 2017, disponível em http://dx.doi.org/10.1080/13600834.2017.1301036.
40 Cf. S. NAKAMOTO, *op. cit.*.
41 Cf. L. ALTER (2017). 'Forget Bitcoin; it's the blockchain that might change everything.' Obtido em 15 de Dezembro de 2017, disponível em https://www.treehugger.com/economics/forget-bitcoin-its-blockchain-might-change-everything.html e D. TAPSCOTT & A. TAPSCOTT, *op. cit.*, pp. 7 e 152 *et seq*..
42 Cf. A. BROKAW (2014). *Coindesk*. Obtido em 3 de Novembro de 2017, disponível em https://www.coindesk.com/crypto-2-0-roundup-bitcoins-revolution-moves-beyond-currency/.
43 Cf. V. BUTERIN (2015a). *Ethereum Github*. Obtido em 3 de Novembro de 2017, disponível em https://github.com/ethereum/wiki/wiki/White-Paper.
44 Cf. Nxt Community (2014). *Nxt Whitepaper*. Version 1.2.2. Obtido em 22 de Janeiro de 2018, disponível em https://www.dropbox.com/s/cbuwrorf672c0yy/NxtWhitepaper_v122_rev4.pdf.

de moeda, instrumentos financeiros ou câmbios personalizados (tradução livre de *colored coins*)[45], a propriedade de determinado bem físico (a chamada *smart property*)[46], ou até mesmo votos num sistema de votação electrónica[47], sendo todas as transacções feitas registadas no *blockchain* da plataforma.

Os supramencionados *smart contracts* (ou contratos inteligentes, numa tradução livre), compreendem uma denominação que poderá induzir a erro. Na verdade, SZABO[48] frisa que a adopção do termo '*smart*' (ou inteligente na nossa tradução), não implica necessariamente o recurso à inteligência artificial, mas antes pretende indicar que aquele contrato é dotado de determinadas funções/capacidades que, devido à sua natureza intrínseca, os contratos tradicionais não possuem. Assim, SZABO define um contrato inteligente como um conjunto de promessas expressas em formato digital, onde se incluem as condições/cláusulas que devem ser respeitadas para que o compromisso se realize.

Embora aparentemente irrisório, é possível dizer que uma máquina automática de vendas realiza *smart contracts* primitivos, na medida em que a máquina está programada para dispensar determinado bem, após verificar que a totalidade do preço foi inserida pelo utilizador[49]. Como bem se sabe, esta modalidade de venda encontra-se prevista nos artigos 22.º e seguintes do DL n.º 24/2014, de 14 de Fevereiro. Contudo, será correcto afirmar que aos *smart contracts* se aplicaria por analogia o disposto neste

45 Sobre o termo *colored coins*, cf. Y. ASSIA, V. BUTERIN, M. ROSENFELD & R. LEV (2012). *Colored Coins Whitepaper*. Obtido em15 de Dezembro de 2017, disponível em https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit#heading=h.wxrvzqj8997r.

46 Sobre o conceito de *smart property*, cf., designadamente, N. SZABO (1997). *The Idea of Smart Contracts*, Obtido em 14 de Dezembro de 2017, disponível em http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html; BITCOINWIKI (2016). *Smart Property*. Obtido em 15 de Dezembro de 2017, disponível em https://en.bitcoin.it/wiki/Smart_Property.

47 Sobre o sistema de votação electrónica baseado na tecnologia *blockchain*, cf., ente outros, I. KUBJAS (2017). Using blockchain for enabling internet voting. Obtido em 15 de Dezembro de 2017, disponível em https://courses.cs.ut.ee/MTAT.03.323/2016_fall/uploads/Main/004.pdf, A. BARNES, C. BRAKE & T. PERRY (2016). 'Digital Voting with the use of Blockchain Technology.' Obtido em 15 de Dezembro de 2017, disponível em https://www.economist.com/sites/default/files/plymouth.pdf, F. CAIAZZO (2016). 'A Block-Chain Implemented Voting System.' Obtido em 15 de Dezembro de 2017, disponível em http://www.cs.tufts.edu/comp/116/archive/fall2016/fcaiazzo.pdf.

48 Cf. N. SZABO (1996). *Smart Contracts: Building Blocks for Digital Markets.* Obtigo em14 de Dezembro de 2017, disponível em http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

49 Sobre a equiparação das máquinas automáticas a *'smart contracts* primitivos', cf., entre outros, P. BAILIS & H. Song (2017). 'Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts; Hardware for Deep Learning.' *Communications of the ACM*. 60(5), p. 50; N. SZABO (1996), *op. cit.* e N. SZABO (1997), *op. cit.*.

diploma? Não nos parece. Como nota SZABO[50], *«[s]mart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means*». No mesmo sentido, SAVELYEV[51] refere que as máquinas de venda automática apenas substituem a 'acção humana' de uma das partes, exigindo-se alguma intervenção da outra parte (v.g. inserção de moedas, ou uso de algum meio de pagamento). Por sua vez, *smart contracts* idealizam uma total autonomização da acção humana, manifestando-se uma nova característica daquele contrato. Desta forma, não nos parece razoável subsumir este na definição disposta no diploma anterior.

4.2.Noção e tipos de agentes de *software*

Antes de propormos uma noção de agente de *software*, importa desde logo referir que também aqui se verifica uma denominação indutora de erro, ainda que, desta vez, o lapso seja por conta da tradução e não da escolha de termos: enquanto o termo *smart contracts* foi escolhido por autores que optaram pelo uso indiscriminado de termos jurídicos[52], a expressão 'agente de *software*' trata-se de uma tradução literal do inglês '*software agents*', sendo que o termo '*agent*' no direito anglo-saxónico se aproxima mais da nossa figura de 'representante' ou 'procurador' do que do nosso 'agente', pelo que não podemos compreender estes agentes no sentido técnico que é dado entre nós.

Assim, e embora não exista consenso quanto à definição de agentes de *software*[53], podemos adiantar que se tratam de programas de computador que assistem um sujeito

50 Cf. N. SZABO (1997), *op. cit.*.
51 Cf. A. SAVELYEV, *op. cit.*.
52 Neste sentido, cf. E. MIK (2017). 'Smart contracts: terminology, technical limitations and real world complexity.' *Law, Innovation and Technology*, 9(2). pp. 272-274. Obtido em 30 de Janeiro de 2018, disponível em, https://doi.org/10.1080/17579961.2017.1378468.
53 Sobre a definição de agentes de *software*, cf. M. BURGIN & G. Dodig-Crnkovic (2009) *A Systematic Approach to Artificial Agents*. Obtido em 15 de Dezembro de 2017, disponível em https://arxiv.org/pdf/0902.3513.pdf; S. FRANKLIN & A. GRAESSER (1996). *Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents*. Obtido em 15 de Dezembro de 2017, disponível em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.589.5192&rep=rep1&type=pdf; J. JANSEN (1997). *Using Intelligent Agents to Enhance Search Engine Performance*. Obtido em 15 de Dezembro de 2016, disponível em http://firstmonday.org/ojs/index.php/fm/article/view/517/438; H. NWANA & D. NDUMU (2012). A Brief Introduction to Software Agent Technology.' *Agent Technology: Foundations, Applications, and Markets*. p. 31; P. JANCA & D. GILBERT (2012). 'Practical Design of Intelligent Agent Systems.' *Agent Technology: Foundations, Applications, and Markets*, p. 75; T. ALLEN & R. WIDDISON (1996). 'Can computers make contracts?' *Harvard Journal of Law & Technology*, 9(1), p. 27; P. MAES, R. GUTTMAN & A. MOUKAS (1999). 'Agents that Buy and Sell: Transforming Commerce as we Know It.' *Communications of the ACM* 42(3), p. 1; J. LEROUGE (2000). 'The

utilizador de modo contínuo e autónomo, realizando certa(s) tarefa(s) ou procurando atingir determinado(s) objectivo(s) definidos pelo mesmo. Esta autonomia e continuidade de funcionamento destes agentes permite distingui-los dos comuns programas de computador que tão bem conhecemos.

Sendo possível distinguir diversos tipos de agentes de *software*, interessam-nos especialmente os agentes autónomos e os oráculos: enquanto os agentes autónomos (ou agentes de *software stricto sensu*) dizem respeito a agentes de *software* que residem no *blockchain* e são responsáveis pela execução do seu código (*rectius* a vontade do sujeito utilizador), os oráculos são agentes de *software* instalados em servidores externos que, de modo contínuo e autónomo, verificam e registam determinado tipo de dados no *blockchain*[54], funcionando, portanto, como 'pontes' entre o *blockchain* e o mundo externo. Os oráculos podem ainda ser de *software* (quando lidam com dados disponíveis no ciberespaço externo/para além daquela plataforma) ou *hardware* (quando lidam com dados disponíveis no mundo externo físico), e *inbound* (quando carregam informação do mundo externo para a plataforma) ou *outbound* (quando enviam um comando/instrução da plataforma para o mundo externo, como resultado da operação *output*[55]).

Partindo da definição anterior, facilmente se compreende a razão de BUTERIN[56] ter optado pela designação 'agentes autónomos' ao invés de 'contratos (inteligentes) ',

---

Use of Electronic Agents Questioned under Contractual Law: Suggested Solutions on a European and American level.' *John Marshall Journal of Information Technology & Privacy Law* 18(2), p. 405; I. KERR (2001). 'Ensuring the Success of Contract Formation in Agent-Mediated Electronic Commerce.' *Electronic Commerce Research* 1 (1), pp. 183-184; A. MOUKAS, R. GUTTMAN & P. MAES (2000). *Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective*, pp. 1-2. Obtido em 18 de Janeiro de 2018, disponível em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.335.8810&rep=rep1&type=pdf; T. HABIBZADEH (2016). 'Analysing Legal Status of Electronic Agents Is Contracting through Interactive Websites: Comparative Study of American, English and EU Laws Developing Iranian Legal System.' *Information & Communications Technology Law* 25(2), p. 153. Obtido em 17 de Dezembro de 2017, disponível em http://www.ulcc.ca/en/annual-meetings/359-1999-winnipeg-mb/civil-section-documents/362-providing-for-autonomous-electronic-devices-in-the-electronic-commerce-act-1999?showall=1&limitstart=; entre outros.

54 Cf. BITFURY GROUP (2015). *Smart Contracts on Bitcoin Blockchain*. Obtido em 14 de Dezembro de 2017, disponível em http://bitfury.com/content/5-white-papers-research/contracts-1.1.1.pdf, CHAINFROG OY (2017). *What are Smart Contracts*. Obtido em 14 de Dezembro de 2017, disponível em http://www.chainfrog.com/wp-content/uploads/2017/08/smart-contracts.pdf, WE.USE.CASH (2017). *Dumb Contracts and Smart Scripts*. Obtido em 14 de Dezembro de 2018, disponível em http://weuse.cash/2017/08/15/dumb-contracts-and-smart-scripts/, BLOCKCHAINHUB (s.d.). *Blockchain Oracles*. Obtido em 14 de Dezembro de 2017, disponível em https://blockchainhub.net/blockchain-oracles e E. LARCHEVÊQUE (2016). *Hardware Pythias: bridging the Real World to the Blockchain*. Obtido em 14 de Dezembro de 2017, disponível em https://www.ledger.fr/2016/08/31/hardware-pythias-bridging-the-real-world-to-the-blockchain/#.2zeggzh6f.

55 V. *infra* Figura 3 – O conceito de *blockchain* AirBnB, onde a operação *output* está representada na operação [5], sendo o oráculo neste exemplo a porta inteligente.

56 Cf. V. BUTERIN (2015a), *op. cit.*.

uma vez que, neste contexto, o contrato vai-se cumprindo à medida que o código do agente autónomo é executado – código este que representa a 'vontade' do sujeito utilizador e que, por sua vez, compreende as condições/cláusulas que devem ser respeitadas pelo agente na execução das suas tarefas[57]. Por fim, acrescente-se que estes contratos são identificados por um endereço (representados por um identificador de 160 *bits*), sendo a sua correcta execução garantida por via de um protocolo de consenso, e que, uma vez cumprido o seu propósito, o agente de *software* – *rectius*, o contrato inteligente – caduca e desaparece.

Sendo assim, é concebível que um agente de *software* seja codificado para realizar uma compra e venda, verificando a legitimidade do pretenso vendedor (impedindo a venda de coisa alheia) e a disponibilidade económica do pretenso comprador, garantindo a efectiva entrega do bem caso as condições se verifiquem. O exemplo descrito na Figura 1, representa uma situação que conta com a intervenção de apenas um tipo de agente de *software*.

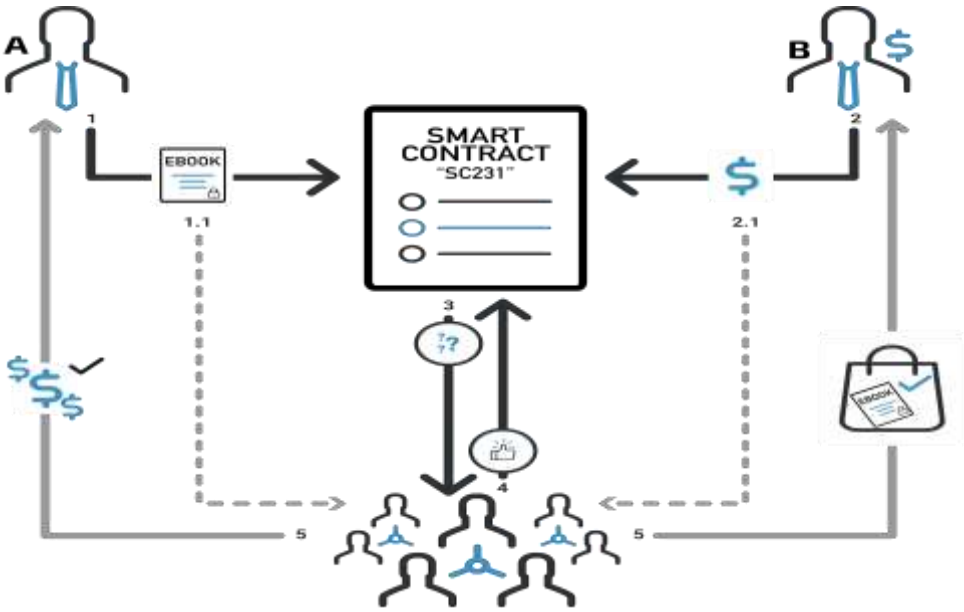

Figura 1 – Compra e venda numa plataforma blockchain

Na Figura 1, André **[A],** que pretende vender um *e-book* por 15 € e que se identifica com o endereço *blockchain* 614494 (chave pública), cria o *smart contract*

57 Relativamente à 'vontade' do agente de *software* e do seu sujeito utilizador, v. infra §4.3 Qualificação jurídica dos agentes de *software.*

"SC231" com os termos e condições da venda (assinando-o digitalmente com a sua chave privada e registando-o no *blockchain*, ficando visível a todos os sujeitos utilizadores da plataforma) **[1]**, e carrega o *e-book* na plataforma, que passa a deter o endereço *blockchain* 3800K1, onde fica armazenado **[1.1];** Bruno **[B]**, que pretende comprar o *e-book* 3800K1, subscreve o *smart contract* **"SC231"** com a sua chave privada, transferindo 15 **€** do seu endereço *blockchain* (chave pública) 778956 para o endereço *blockchain* de André 614494 **[2]**, ficando esta transferência registada no *blockchain* **[2.1]** (operação *input*); posteriormente o agente verifica se André tem legitimidade para vender o *e-book*, se Bruno detém crédito suficiente para efectuar a compra, e se o pagamento foi efectuado **[3]**. Sendo todas as condições favoráveis, **[4]**, inicia-se a operação de *output*, concedendo a Bruno um ponto de descarga do *e-book* 3800K1, e disponibilizando-se o valor de 15 € na conta de André, transferidos da conta de Bruno **[5]**[58].

Na Figura 2 é representado um exemplo de uma aposta inscrita num *blockchain* cujo resultado depende de dados externos, sendo necessário recorrer a dados obtidos por um oráculo.

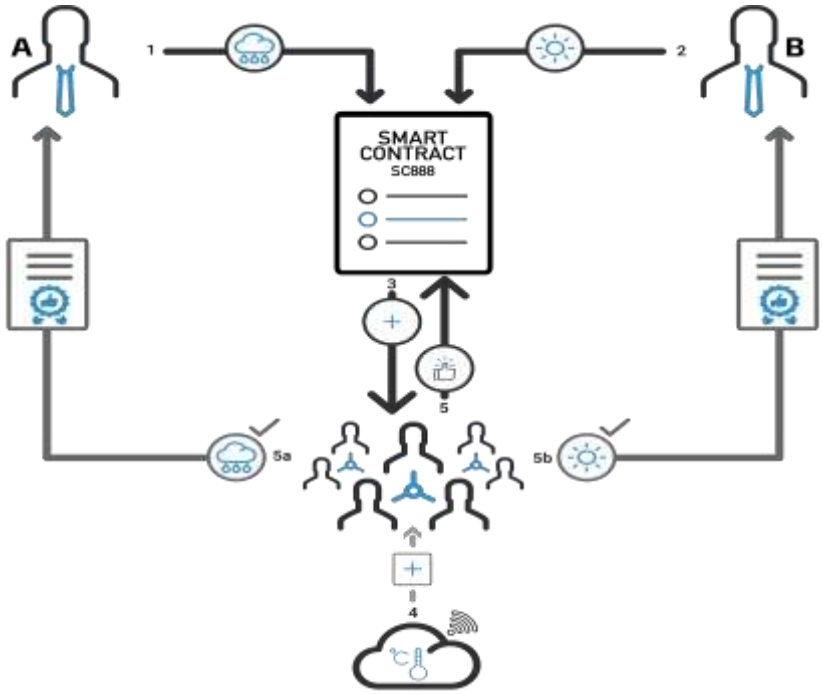

Figura 2 – Inscrição de uma aposta em blockchain

58 Cf. L. Luu, D. Chu, H. Olickel, P. Saxena & H. Aquinas (2016). 'Making Smart Contracts Smarter.' *CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 254-256.

Na Figura 2, Antero **[A]** e Bento **[B]** criam uma aposta sobre o estado meteorológico de Coimbra no dia 1 de Abril de 2018: para A choveria nesse dia **[1]**, para B estaria um dia radiante de sol **[2]**. Esta aposta é inscrita num *smart contract* que é registado na plataforma *blockchain* **[3]**. A execução do código deste contrato consiste na monitorização, por parte do agente autónomo, dos dados meteorológicos submetidos pelo oráculo de *hardware inbound* do Instituto Português do Mar e da Atmosfera, que são contínua e autonomamente registados no *blockchain* **[4]**. Verificada a data e as condições meteorológicas no dia 1 de Abril de 2018 **[5]**, o agente autónomo atribui o prémio a A **[5a]** ou a B **[5b]**, emitindo um documento electrónico com essa informação.

Por fim, na Figura 3 é exibido um exemplo de uma plataforma de pesquisa e reserva de alojamentos locais particulares, semelhante ao AirBnB[59], operado com recurso a *blockchain* ('bAirBnB')[60], uma plataforma destinada ao apresentar uma listagem de imóveis disponíveis para arrendamento a curto prazo. Neste exemplo, o oráculo corresponde a uma porta inteligente que permite o acesso ao imóvel/divisão do imóvel quando se verifique que estão reunidas as condições acordadas entre as partes.

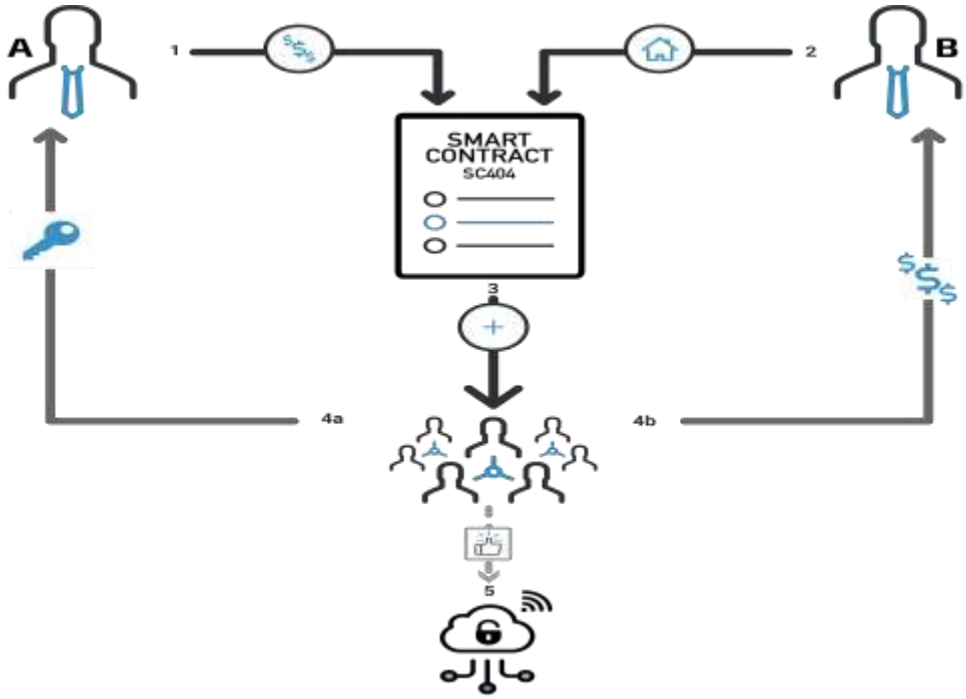

Figura 3 – Representação do 'blockchain AirBnb'

59 Sobre o AirBnB, cf. AirBnB: http://www.airbnb.pt.
60 Cf. D. TAPSCOTT & A. TAPSCOTT, *op. cit.*, pp. 115-117.

Na Figura 3, Artur **[A]** e Benjamim **[B]** já se encontram inscritos na plataforma 'bAirBnB'. A, interessado em ficar alojado no imóvel disponibilizado por B, procede ao pagamento do depósito exigido, apresentando o documento comprovativo **[1]**. Perante a proposta de A e pretendendo aceitá-la, B valida e autoriza a reserva do imóvel **[2]**. Estes actos são todos inscritos num *smart contract* que por sua vez é registado no *blockchain* **[3]**. Verificando-se todas as condições do contrato, a chave do imóvel é entregue a A, no formato de um código QR **[4a]**, sendo disponibilizado o valor pecuniário a B **[4b]**. Assim, quando A pretender entrar no imóvel, deverá apresentar a 'chave QR' do imóvel no leitor óptico da fechadura da porta inteligente para abri-la. Assim, se a porta inteligente (*rectius* o oráculo) verificar que ainda estão reunidos os pressupostos que legitimam a entrada no imóvel, o trinco da porta é desbloqueado **[5]**.

Sendo cogitável que as partes pudessem ter interesse em que os seus contratos persistissem mesmo após a sua execução, e desejando inclusivamente que o agente de *software* do contrato interagisse com outros agentes de *software* e/ou oráculos, pensou-se numa figura associada aos contratos inteligentes: a 'organização autónoma descentralizada' (do inglês *decentralized autonomous organization*). HEARN[61] idealizou um futuro onde veículos sem condutor transportariam passageiros que pagariam a viagem electronicamente e, depois de deixar o passageiro no seu destino, dirigir-se-iam a uma bomba de abastecimento para reabastecer, utilizando o valor pecuniário guardado na *sua* carteira electrónica. Além disso, o veículo poderia, por sua iniciativa, contratar um terceiro para efectuar algum tipo de reparação/manutenção, pagando igualmente por via electrónica. No entender do autor, neste cenário, o veículo é dono de si próprio, *rectius*, é efectivamente uma organização autónoma descentralizada. Se este cenário se concretizasse, aproximar-nos-íamos de organizações mais eficientes, económicas e competitivas, quando comparadas às tradicionais empresas do mercado real. Contudo, ressalte-se que o cenário que se apresenta remete para o campo da inteligência artificial e da condução autónoma que, não obstante se trate de uma realidade notavelmente actual e intensamente debatida[62], para o trabalho que desenvolvemos, não tem interesse.

61 Cf. M. HEARN (2013). *Autonomous agents, self driving cars and Bitcoin*. Obtido em 4 de Novembro de 2017, disponível em https://www.youtube.com/watch?v=MVyv4t0OKe4.

62 Sobre os veículos autónomos, v., por exemplo nos meios de comunicação social, ANTÓNIO, F. (2017). 'Táxi autónomo. Continental aponta à Uber e Google.' *Observador*. Obtido em 28 de Janeiro de 2018, disponível em http://observador.pt/2017/07/26/taxi-autonomo-continental-aponta-a-uber-e-google/, B. STRAIGHT (2018). 'Toyota introduces autonomous freight concept vehicle.' Obtido em 28 de Janeiro de 2018, disponível em

5.CONTRATAÇÃO ELECTRÓNICA

5.1. Abordagem ao tema e modalidades de contratação electrónica

Situando-nos presentemente na Era da Informação, assiste-se a uma crescente mitigação de distâncias entre pessoas através da tecnologia; trata-se, pois, de um resultado dos avanços tecnológicos provenientes da Terceira Revolução Industrial, mais concretamente da evolução e expansão da Internet. A renomada *network of networks*, trazendo consigo uma nova forma de comunicação mais eficiente, cómoda e económica, não passou despercebida aos prestadores de bens e serviços e a potenciais consumidores, que rapidamente a adoptaram para fins comerciais[63]. Foi precisamente a facilidade e a rapidez de processamento e transmissão electrónicos de dados, que permitiu a negociação executada por meios electrónicos e o aparecimento do comércio electrónico[64].

---

https://www.freightwaves.com/news/toyota-shows-autonomous-freight-vehicle, A. HAWKINS (2017). 'Uber is getting serious about building real, honest-to-god flying taxis.' *CNBC.* Obtido em 28 de Janeiro de 2018, disponível em https://www.cnbc.com/2017/04/25/uber-reveals-plans-for-flying-taxis-at-elevate-event.html, A. KHARPAL (2017). 'NASA is working with Uber on its flying taxi project.' *CNBC.* Obtido em 28 de Janeiro de 2018, disponível em https://www.cnbc.com/2017/11/08/uber-nasa-work-on-flying-taxis.html.
Sobre o desenvolvimento da inteligência artificial, cf. ALPHAGO URL, disponível em https://deepmind.com/research/alphago/ (Obtido em 28 de Janeiro de 2018), e nos meios de comunicação social, designadamente, M. ALBERTSON (2018). *Artificial intelligence gets smarter at predicting what's coming next*. Obtido em 28 de Janeiro de 2018, disponível em https://siliconangle.com/blog/2018/01/27/artificial-intelligence-gets-smarter-predicting-whats-coming-next/, SCMP (2018), D. HARWELL (2018). 'Shake-up at Facebook highlights tension in race for AI.' *Washington Post.* Obtido em 28 de Janeiro de 2018, disponível em https://www.washingtonpost.com/business/economy/shake-up-at-facebook-highlights-tension-in-race-for-ai/2018/01/24/5d21239a-0138-11e8-9d31-d72cf78dbeee_story.html?utm_term=.ba531f130398, M. WEHNER (2017). *Facebook engineers panic, pull plug on AI after bots develop their own language.* Obtido em 28 de Janeiro de 2018, disponível em http://bgr.com/2017/07/31/facebook-ai-shutdown-language/, S. BHATIA (2018). *Teaching Artificial Intelligence to teach itself*. Obtido em 28 de Janeiro de 2018, disponível em http://www.livemint.com/Leisure/vtiKX8KtqZ97zjbB3M2q3N/Teaching-Artificial-Intelligence-to-teach-itself.html.

63 Cf. P. SILVA (1999). 'Transferência electrónica de dados: a formação dos contratos'. *Direito da Sociedade da Informação*, Vol. I. p. 216; J. ASCENSÃO (2004), *in* O Comércio Electrónico em Portugal: O quadro legal e o negócio. *ANACOM*. p. 157. Obtido em 19 de Dezembro de 2017, disponível em https://www.anacom.pt/streaming/manual_comercio_elec.pdf?contentId=178219&field=ATTACHED_FILE.

64 O comércio electrónico pode ser definido como o conjunto de operações materiais e actos jurídicos concluídos ou praticados por via do processamento e transmissão electrónicos de dados. Sobre o conceito de contratação electrónica, cf., entre outros, D. VICENTE (2003). 'Comércio electrónico e resposabilidade empresarial.' *Direito da Sociedade da Informação*, Vol. IV, p. 241; A. L. PEREIRA (1999a), *Comércio Electrónico na Sociedade da Informação: Da segurança técnica à confiança jurídica*. p. 14; I. Galvão TELLES (2002). *Manual dos contratos em geral : refundido e actualizado*, 4ª Edição. pp. 151-153; P. SILVA (2003). 'A contratação automatizada'. *Direito da Sociedade da Informação*, Vol. IV, p. 290.

Diversas realidades foram antecipadas no Livro Verde para a Sociedade da Informação, nomeadamente a realidade do comércio electrónico, prevendo o ponto §5.7 que «[a] globalização dos mercados obriga as empresas a repensar e modificar os seus processos empresariais por forma a adaptá-los à nova realidade envolvente. Neste contexto, o comércio electrónico surge como uma ferramenta estratégica para esta redefinição dos processos de negócio, muitas vezes catalisando essa globalização. As empresas que aderem a este conceito pretendem tornar mais flexíveis e eficientes as suas actividades associadas à comercialização, alargar a sua base de clientes, e melhorar a resposta às expectativas dos seus parceiros comerciais»[65]. Estas afirmações não poderiam ser mais actuais, reportando para uma realidade indubitavelmente palpável.

Entre nós, a contratação electrónica encontra-se regulada no DL n.º 7/2004, de 7 de Janeiro (com as alterações dadas pelo DL n.º 62/2009, de 10 de Março, e pela Lei n.º 46/2012, de 29 de Agosto), que procedeu à transposição da Directiva n.º 2000/31/CE, de 8 de Junho[66]. O preceituado deste Diploma pretende abranger «todo o tipo de contratos, sejam ou não qualificáveis como comerciais», como se lê no Preâmbulo do mesmo, sendo subsidiariamente aplicável, nomeadamente, o disposto no DL n.º 24/2014, de 14 de Fevereiro, com as alterações da Lei n.º 47/2014, de 28 de Julho[67–68]. É também aplicável o Regulamento (UE) n.º 910/2014, de 23 de Julho, relativo à identificação electrónica e aos serviços de confiança para as transacções electrónicas no mercado interno, que veio revogar a Directiva 1999/93/CE, e que tem em vista o reforço da confiança nas transacções electrónicas, bem como a Recomendação da Comissão 94/820/CE, de 19 de Outubro, relativa aos aspectos jurídicos da transferência electrónica de dados.

Como nota ASCENSÃO[69], é na tendencial equiparação plena da contratação electrónica (e contratação informática) à contratação comum que encontramos a nossa

65 Cf. Ministério da Ciência e da Tecnologia (1997). *Livro Verde para a Sociedade da Informação em Portugal*, p. 47.
66 Doravante 'DCE'.
67 Note-se que a Directiva sobre contratos à distância (Directiva 97/7/CE, do Parlamento Europeu e do Conselho, de 20 de Maio) foi transposta para a ordem jurídica interna através do DL n.º 143/2001, de 26 de Abril. Contudo, tendo aquela sido revogada pela Directiva relativa aos direitos dos consumidores (Directiva 2011/83/UE, do Parlamento Europeu e do Conselho, de 25 de Outubro), foi o nosso DL n.º 143, 2001, de 26 de Abril, revogado pelo DL n.º 24/2014, de 14 de Fevereiro, que transpõe a aludida Directiva relativa aos direitos dos consumidores.
68 Cf. Ministério da Justiça: Gabinete de Política Legislativa e Planeamento (2005). *Lei do Comércio Electrónico Anotada*, p. 94.
69 Cf. J. ASCENSÃO (2004),*op. cit.*, p. 104.

base jurídica elementar. E dizemos tendencial devido à exclusão de determinados domínios, como se retira do prescrito no n.º 2 do artigo 9.º da DCE, no n.º 3 do artigo 3.º da Directiva 2011/83/EU, de 25 de Outubro[70], e no artigo 2.º da LCE. O autor adianta ainda que o contrato electrónico se trata de um contrato celebrado à distância por meios electrónicos, podendo este entendimento ser retirado da nota (20) do preâmbulo da DCD. Assim, justifica-se a aplicação dos princípios relativos à contratação à distância aos contratos electrónicos (e informáticos), salvo disposição legal em contrário, implicando igualmente a vigência dos deveres de informação inerentes àqueles na contratação electrónica (e informática).

Apresentado o tema da contratação informática, mas antes de passar ao cerne da nossa investigação, cumpre-nos identificar as modalidades da contratação electrónica. Dado que estaremos perante a forma electrónica de contratação quando as declarações de vontade das partes sejam transmitidas por meios electrónicos, é possível afirmar que o conceito de contratação electrónica será mais amplo ou mais restrito conforme os meios tecnológicos empregues durante os actos de processamento e transmissão daquelas[71]. Assim, por um lado, quando para a conclusão do negócio jurídico seja exigível intervenção humana no momento da celebração do negócio jurídico, diremos que estamos perante **contratação electrónica *stricto sensu***: nesta modalidade os aparelhos electrónicos são utilizados única e exclusivamente como meios de comunicação (v.g. contratação efetuada por correio electrónico); por outro, quando aquela intervenção seja inexigível, visto que os contratos são celebrados e formados (unilateral ou bilateralmente) por computador(es), já se denominará como **contratação electrónica automatizada**[72], ou somente contratação automatizada.

Como facilmente se depreende, cabe na contratação electrónica automatizada a contratação com recurso à transferência electrónica de dados (TED, na sigla portuguesa, ou *electronic data interchange*, EDI, na sigla inglesa), que já foi definida de diversas maneiras[73]. Das diferentes definições, é possível destacar três elementos comuns que

70 Doravante 'DCD'.
71 Cf. D. FESTAS (2006). 'A contratação electrónica automatizada.' *Direito da Sociedade da Informação,* Vol. VI, p. 412 (nota 3).
72 No mesmo sentido, cf. D. FESTAS, *op. cit.*, pp. 412-417; P. SILVA (2003), *op. cit.*, p. 290. Em sentido diverso, cf., nomeadamente, ASENSIO *apud* D. FESTAS, *op. cit., loc. cit.*, que distingue a contratação automatizada (contratação electrónica em sentido estrito) da contratação por meios electrónicos.
73 O artigo 2.2 da atEDI define a EDI como «[t]ransferência eletrónica, de computador para computador, de dados comerciais e administrativos utilizando uma norma acordada para estruturar uma mensagem EDI». Para mais

caracterizam a EDI: (i) o formato electrónico estruturado e estandardizado, (ii) a capacidade de partilhar dados, de modo legível, entre (pelo menos dois) computadores situados em locais diversos, e (iii) a inexigibilidade de intervenção humana para receber (e interpretar) e (inserir e) enviar os dados.

Apesar da conveniência, rapidamente se identificaram alguns contratempos na contratação com recurso à EDI (que, por sua vez, dificultavam a sua adesão): além de um avultado investimento na aquisição da tecnologia, associada à contratação automatizada com recurso à EDI esteve sempre a exigência de celebração de complexos acordos prévios (onde são estabelecidos diversos aspectos da contratação por forma a garantir o «ambiente operacional para pôr em funcionamento o EDI»[74]). Perante isto, o desenvolvimento desta conheceu diversas recomendações (nacionais, internacionais e institucionais) cujo desiderato era a simplificação e estandardização das normas utilizadas nos sobreditos acordos-prévios, proporcionando uma redução ou eliminação de obstáculos jurídicos e da ambiguidade no comércio electrónico, que se traduziram em modelos de acordos de intercâmbio (do inglês *interchange agreements*)[75] e que deveriam ser adoptados pelas partes. Como nota FESTAS[76], a adopção da contratação automatizada com recurso à EDI foi especialmente relevante em determinadas indústrias, nomeadamente na indústria automóvel, na actividade bancária e seguradora, na negociação em bolsa[77], e no sector da distribuição.

---

interpretações, cf., entre outros, N. HILL & D. FERGUSON (1989). 'Electronic Data Interchange: A definition and perspective.' *The Journal of Electronic Commerce* 1(1), p. 6; R. O'CALLAGHAN, P. KAUFMAN & B. KONSYNKI (1992). 'Adoption correlates and share effects of Electronic Data Interchange systems in marketing channels.' *Journal of Marketing* 56 (2), p. 46; D. UPTON & A. MCAFEE (1996). 'The Real Virtual Factory.' *Harvard Business Review* (July-August), p. 125; S. WALTON & A. MARUCHECK (1997). 'The Relationship Between EDI and Supplier Reliability.' *International Journal of Purchasing and Materials Management* Summer (33), p. 31; J. FISCHER (1997). 'Computers as Agents: A Proposed Approach to Revised U.C.C. Article 2.' *Indiana Law Journal* 72 (2), pp. 547-550; P. FINNEGAN, W. GOLDEN & D. MURPHY (1998). 'Implementing Electronic Data Interchange: A Nontechnological Perspective.' *International Journal of Electronic Commerce* 2 (4), p. 28; S. ANDERSON & W. LANEN (2002). 'Using Electronic Data Interchange (EDI) to Improve the Efficiency of Accounting Transactions.' *The Accounting Review* 77 (4), p. 704; D. FESTAS, *op. cit.*, p. 414 (nota 9); A. ASHER (2007). 'Developing a B2B E-Commerce Implementation Framework: A Study of EDI Implementation for Procurement.' *Information Systems Management* 24 (4), p. 375.

74 Cf. artigo 9.1 da atEDI.

75 Relativamente aos modelos de acordo de intercâmbio, destacamos o Modelo Europeu de Acordo de EDI (atEDI), as *Uniform Rules of Conduct for Interchange Trade of Data by Teletransmission* (UNCID) da Câmara de Comércio Internacional, o *Model Trading Partner Agreement* da *American Bar Association*, o *EDI-Modellvertrag* (que resultou do projecto de investigação ELTRADO – *Elektronische Transaktion von Dokumenten zwischen Organisationen*) e a Lei-Modelo da Comissão das Nações Unidas para o Direito da Comércio Internacional sobre o Comércio Electrónico, de 1996.

76 Cf. D. FESTAS, *op. cit.*, p. 415 (nota 9).

77 Cf. D. D. WONG (1999). 'The Emerging Law of Electronic Agents: E-Commerce and Beyond...' *Suffolk University Law Review* XXXIII, p. 90.

Todavia, a evolução da contratação electrónica automatizada conta hoje, não apenas com a contratação com recurso à EDI, mas também com a contratação com recurso a agentes electrónicos. Com efeito, em 2005, na Convenção das Nações Unidas sobre o Uso de Comunicações Electrónicas em Contratos Internacionais[78–79], consagrou-se a possibilidade de contratar com recurso a sistemas automatizados de mensagens (do inglês *automated message systems*), também conhecidos como «agentes electrónicos»[80]. Ou seja, através de um programa de computador (ou outro meio automatizado electrónico) utilizado para iniciar uma acção ou responder a operações ou mensagens de dados, e que dispensa, total ou parcialmente, a intervenção de uma pessoa humana de cada vez que se inicia uma acção e/ou quando seja gerada uma resposta pelo sistema, como é definido na Convenção[81]. Na verdade, e como denota FESTAS[82], os agentes electrónicos, dotados de uma versatilidade que lhes permite executar diversas funções, tratam-se de um instrumento relevantíssimo para o comércio, podendo adoptar diferentes nomenclaturas conforme a sua função. Dito de outra forma, serão agentes electrónicos os *search agents*, os *filtering agents*, os *shopping agents* e os *broker agents*, já que a sua função é pesquisar, filtrar, adquirir e negociar, respectivamente, sendo possível identificar muitos outros agentes com funções distintas. Por conseguinte, cremos que a definição de agentes electrónicos adiantada pela Convenção se identifica com a supracitada noção de agentes de *software*[83].

78 A Convenção das Nações Unidas sobre o Uso de Comunicações Electrónicas em Contratos Internacionais, adoptada pela Assembleia Geral das Nações Unidas em Nova Iorque a 23 de Novembro de 2005 através da Resolução 60/21, teve em vista, sem se imiscuir na legislação de cada Estado relativo ao regime substantivo dos contratos (cf. artigos 7.º e 13.º da Convenção), a fixação de um regime legal aplicável à contratação internacional efectuada por meios electrónicos. Nos termos do artigo 4 daquela, diz-se comunicação electrónica aquela que se processa por meio de transmissão de mensagens de dados por meios electrónicos, ópticos, magnéticos, ou equivalente, incluindo-se aqui também a correspondência electrónica de dados, o correio electrónico, o telegrama, o telex ou a telecópia. Entre nós, encontramos na Lei n.º 5/2004, de 10 de Fevereiro, recentemente alterada pelo DL n.º 92/2017, de 31 de Julho, a definição de «rede de comunicações electrónicas» na alínea dd) do artigo 3º.

79 Doravante 'Convenção'.

80 Cf. Notas explicativas da Convenção das Nações Unidas sobre o Uso de Comunicações Electrónicas em Contratos Internacionais, p. 69, §208.

81 Cf. alínea g) do artigo 4.º da Convenção.

82 Cf. D. FESTAS, *op. cit.*, p. 415 (nota 9).

83 V. *supra* §3.2 – Noção e tipos de agentes de *software.*

5.2 Caracterização dos *agentes de software*

Tendo-se verificado que o agente de *software* é, a bem dizer, um agente electrónico, é necessário esclarecer que a actividade dos agentes de que temos falado se traduz na celebração de contratos (tipicamente 'em nome' de uma pessoa singular ou colectiva) de modo autónomo e sem intervenção humana, mas agora recorrendo ao uso extensivo de operações criptográficas[84] para conferir maior segurança e confiança, deixando de operar em rede aberta (*rectius* na *World Wide Web*), como se verificava no caso de agentes como o Kasbah[85], o Tête-à-Tête (T@T)[86], ou o AuctionBot[87].

Não obstante, uns e outros partilham determinadas características que os distinguem dos comuns programas de computador que tão bem conhecemos[88], e das quais destacamos as capacidades (i) de actuação autónoma e de autonomia decisória *(autonomy)*[89], (ii) comunicativa *(social ability)*, (iii) de reacção a estímulos *(reactivity)*[90], (iv) de proactividade *(pro-activeness)* e (v) de execução continuada.

84 V. supra §2. A assinatura electrónica.

85 Sobre o agente Kasbah, cf., designadamente, Kasbah URL: https://kasbah.media.mit.edu; P. MAES *et al.*, *op. cit.*, p. 1 e 8-10; I. KERR (2001). 'Ensuring the Success of Contract Formation in Agent-Mediated Electronic Commerce.' *Electronic Commerce Research* 1(1), p. 185; MOUKAS *et al.*, *op. cit.*, p. 3; R. GUTTMAN, A. MOUKAS & P. MAES (1998). 'Agent-mediated Electronic Commerce: A Survey.' *The Knowledge Engineering Review* (Cambridge University Press) 13 (2), pp. 149-151.

86 Sobre o agente Tête-à-Tête (T@T), cf., entre outros, T@T URL: http://ecommerce.media.mit.edu/tete-a-tete/; P. MAES *et al.*, *op. cit.*, pp. 1 e 10; I. KERR (2001), *op. cit.*, pp. 185-186; R. GUTTMAN *et al.*, *op. cit.*, pp. 151.

87 Sobre o agente AuctionBot, cf., nomeadamente, AuctionBot URL: http://auction.eecs.umich.edu; P. MAES *et al.*, *op. cit.*, pp. 1 e 8; R. GUTTMAN *et al.*, *op. cit.*, pp. 150, P. WURMAN, M. WELLMAN & W. WALSH (1998). 'The Michigan Internet AuctionBot: A Configurable Auction Server for Human and Software Agents.' *Second International Conference on Autonomous Agents (Agents-98)*, pp. 301-308.

88 Sobre as características dos agentes electrónicos/agentes de *software*, cf., entre outros, FESTAS, D., op. cit., p. 415 (nota 9); P. JANCA *et al.*, *op. cit.*, p. 75; H. NWANA (1996). 'Software Agents: An Overview.' *Knowledge Engineering Review* 11 (3), pp. 211-212; A. BELLIA JR. (2001). 'Contracting with Electronic Agents.' *Emory Law Journal* 50. p. 1051 (nota 19); S. FRANKLIN *et al.*, *op. cit.*, pp. 21-27; M. WOOLDRIGE, & N. JENNINGS (1995). 'Intelligent agents: theory and practice.' *The Knowledge Engineering Review* 10 (2), pp. 116-117; O. ETZIONI, N. Lesh & R. Segal (1994). 'Building Softbots for UNIX (Preliminary Report).' *AAAI Technical Report* SS-94-04 p. 10; J. FISCHER, *op. cit.*, p. 558; I. KERR, I. (1999). *Providing for Autonomous Electronic Devices in the Electronic Commerce Act 1999*. §I. The technological promise of autonomous electronic devices. Obtido em 26 de Janeiro de 2018, disponível em http://www.ulcc.ca/en/1999-winnipeg-mb/359-civil-section-documents/362-providing-for-autonomous-electronic-devices-in-the-electronic-commerce-act-1999; F. COELHO (2017 – em vias de publicação). 'Contratação automatizada e execução contratual automatizada: dos "software agents" aos "smarts contracts".' *Congresso de Direito e Robótica.* Conferência disponível online em https://www.facebook.com/ij.fduc/videos/1931385373792186/ (obtido em 18 de Novembro de 2017).

89 A autonomia do *softbot* pode ser definida como «capacidade de tomar decisões e de as aplicar no mundo exterior, independentemente do controlo ou da influência externa» (cf. Resolução do Parlamento Europeu de 16 de Fevereiro de 2017, §AA), podendo o grau desta capacidade depender do «nível de sofisticação da interação de um robô com o seu ambiente» (cf. Resolução do Parlamento Europeu de 16 de Fevereiro de 2017, §AA).

90 Por capacidade de reacção a estímulos quer-se dizer a habilidade de recolher e interpretar diversas informações quer do mundo físico (v.g. via oráculos), quer do mundo digital, por forma a adequar/modificar, se necessário, a 'sua' decisão.

Note-se que JANCA & GILBERT[91] enunciam um conjunto de características que são, à primeira vista, distintas daquelas que acabámos de apresentar; no entanto, entende-se que estas se subsumem naquelas, já que o agente de *software*, munido daquelas cinco capacidades, é capaz de encontrar a solução mais adequada para cumprir o fim para o qual foi programado, 'em nome' do seu sujeito utilizador, da forma mais eficiente possível. Com efeito, além de não nos podermos esquecer que o nosso agente é um programa de computador dotado de características específicas, é fundamental compreender que a sua interacção é *personalizável*. Por outras palavras: sabendo que o agente de *software* é um programa de computador destinado a actuar 'em nome' do seu sujeito utilizador autonomamente, o utilizador pode decidir o seu grau de autonomia, e se será ou não, por exemplo, dotado de capacidades de observação de padrões de comportamento e de auto-aprendizagem (e, se for o caso, em que medida) para melhor se adaptar a situações futuras iguais ou semelhantes e, dessa maneira, optar, por uma decisão *melhor* (ou mais *adequada*).

É indiscutível que o código do agente de *software* é concebido por engenheiros humanos e instalado em determinado sistema por um programador humano. Porém, a autonomia característica destes programas de computador verifica-se na medida em que a sua actividade não resulta de uma instrução precisa e inequívoca humana (v.g. comprar a caneta ∂, ao vendedor $\boldsymbol{W}$ que custa 3 €, na Plataforma AlphaBuy); aliás, resulta antes de uma instrução incompleta, mas adequada, dada por um humano para ser completada pelo agente[92] (v.g. comprar a caneta ∂, ao *melhor preço*[93]). Perante uma instrução deste tipo, caberá ao agente preparar, negociar e celebrar o contrato autonomamente, a partir da sua capacidade de análise de dados e autonomia decisória. Não espanta por isto que se equipare estes agentes a robôs de *software* (ou, na expressão abreviada anglo-saxónica, *softbots*). Posto isto, diremos que os interlocutores neste modo de contratação são, precisamente, os aludidos *softbots*.

Pelo exposto depreende-se que, das características que já avançamos dos *softbots*, devemos dar especial ênfase à sua capacidade de autonomia decisória, na medida em

91 Cf. P. JANCA *et al*., *op. cit.*, p. 75.
92 Cf. M. WELLMAN, A. GREENWALD & P. STONE (2007). *Autonomous Bidding Agents*, p. 3; D. FESTAS, *op. cit.*, pp. 422-425.
93 O '*melhor preço*', como se compreende, será um conceito indeterminado que o agente de *software* deverá interpretar, atendendo à instrução que lhe é dada e às informações (do mundo físico e/ou do mundo digital) de que dispõe.

que é esta habilidade que confere ao *softbot* a faculdade de tomar decisões, segundo as instruções do seu sujeito utilizador, em função das informações que vai captando do mundo físico e/ou digital e em nome do seu sujeito utilizador, podendo esta sua autonomia decisória ser personalizada. Desta maneira, no entender de COELHO[94], aos agentes de *software* não compete somente a mera emissão de declarações contratuais; estes serão também portadores de uma «'vontade' negocial», ainda que em formato electrónico[95]. De facto, o agente de *software* prepara, negoceia e celebra contratos, mas executa estas funções 'em nome' (*lato sensu*) do seu sujeito utilizador (que será sempre uma pessoa, singular ou colectiva, titular de uma esfera jurídica, de direitos e obrigações, e de um património responsável).

5.3 Qualificação jurídica dos agentes de *software*

Já se avançou que a EDI permite que programas de computador desencadeiem ordens de encomenda para outros computadores, que por sua vez dão instruções para a execução correspondente, emitindo avisos de recepção no processo de modo automático e sem intervenção humana[96]. Sendo assim, e considerando que a contratação com recurso a *softbots* é uma forma de contratação electrónica automatizada, seria a atEDI igualmente aplicável? Cremos ser razoável responder pela negativa, devido às diferenças entre a contratação com recurso à EDI e a contratação com recurso a *softbots*. Uma das principais características da EDI europeia é o da estandardização da estrutura de comunicação a ser mantida entre as partes, permitindo um ambiente operacional estável e sem ambiguidades por via de um acordo prévio entre as partes, reduzido a escrito (cf. artigos 1.º, 2.º e 9.º atEDI). Do sobredito, evidenciam-se desde logo três diferenças:

94 Cf. F. COELHO, *op. cit.*.
95 Neste sentido, cf., entre outros, D. FESTAS, *op. cit.*, p. 418; A. MONTEIRO (1999). 'A responsabilidade civil na negociação informática'. *Direito da Sociedade da Informação*, Vol. I, pp. 232-233; P. SILVA (2003), *op. cit.*, *passim*.
96 Cf. J. ASCENSÃO (2003a). 'Bases para uma transposição da directriz n.º 00/31, de 8 de Junho (Comércio electrónico).' *Separata da Revista da Faculdade de Direito da Universidade de Lisboa*, XLIV (1 e 2), pp. 63-65, A. L. PEREIRA (1999a), *op. cit.*, pp. 30-32, A. L. PEREIRA (1999b). 'Programas de Computador, Sistemas informáticos e Comunicações electrónicas: alguns aspectos jurídico-contratuais.' *Revista da Ordem dos Advogados* Ano 59 (III), pp. 970-973.

(i) Enquanto na contratação com recurso à EDI as partes conhecem-se antes de iniciarem trocas comerciais, na contratação com recurso a *softbots*, as partes não têm necessariamente de se conhecer previamente;

(ii) Na contratação com recurso à EDI as partes estabelecem entre si um acordo-tipo que definirá o modo como deverão comunicar e contratar, convenção esta que inexiste na contratação com recurso a *softbots*;

(iii) Por fim, tipicamente são grandes empresas que dão uso à contratação com recurso à EDI para comprar ou vender bens ao(s) mesmo(s) sujeito(s); na contratação com recurso a *softbots* os sujeitos intervenientes poderão ser ambos consumidores[97].

Não obstante, ainda que o tipo de contratação electrónica automatizada de que tratamos (*rectius* criptocontratação) convoque a participação de *softbots* e o recurso à criptografia para concluir negócios jurídicos sem intervenção (directa) humana[98], não pode um contrato celebrado por esta via, no nosso ponto de vista, ver os seus efeitos legais negados pelo recurso a este meio. Efectivamente, prescreve o artigo 24.º da LCE que as disposições do capítulo relativo à contratação electrónica se aplicam «a todo o tipo de contratos celebrados por via electrónica ou informática». Contudo, o legislador impôs uma condição subjectiva para os artigos 27.º a 29.º e 34.º, na medida em que se pressupõe que uma das partes seja um prestador de serviços da sociedade da informação[99]. Ao que tudo indica, *prima facie*, os restantes preceitos legais serão aplicáveis a esta forma de contratação.

A análise dos artigos 8.º, 9.º e 12.º da Convenção, bem como dos seus Considerandos, permite-nos depreender que se consagram dois princípios: o princípio da igualdade jurídica dos meios de comunicação e da proibição de discriminação das comunicações por meios electrónicos, e o princípio da liberdade de forma.[100]. Atendendo ao disposto no n.º 1 do artigo 25.º da LCE e no n.º 1 do artigo 9.º da DCE (ambos relativos à contratação electrónica) e no n.º 1 do artigo 25.º, no n.º 1 do artigo 35.º, no n.º 1 do artigo 41.º, no n.º 1 do artigo 43.º e no artigo 46.º, todos do eIDAS

97 Neste sentido, cf., entre outros, S. KIS (2004). 'Contracts and Electronic Agents.' *University of Georgia School of Law*. Obtido em 18 de Dezembro de 2017, disponível em http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1025&context=stu_llm, pp. 15-16; D. FESTAS, *op. cit.*, p. 416 (nota 9).

98 V. supra §2. A assinatura electrónica.

99 Cf. Lei do Comércio Electrónico Anotada, *op. cit.*, pp. 94-95.

100 Neste sentido, D. PEREIRA (2013). 'Princípios gerais da contratação pública electrónica.' *Revista Electrónica de Direito.* Centro de Investigação Jurídico-Económica, pp. 8-9. Obtido em 14 de Janeiro de 2018, disponível em https://www.cije.up.pt/content/princ%C3%ADpios-gerais-da-contratação-pública-electrónica.

(referentes às assinaturas electrónicas, aos selos electrónicos, aos selos temporais electrónicos, ao serviço de envio registado electrónico e aos documentos electrónicos, respectivamente), diremos que também no ordenamento jurídico português se faz alusão a uma proibição de discriminação das comunicações por meios electrónicos, em prol de uma igualdade jurídica dos meios de comunicação e liberdade de forma. Nesta senda, figura-se a consagração do princípio da liberdade de celebração de contratos por via electrónica no n.º 1 do artigo 25.º da LCE e no n.º 1 do artigo 9.º da DCE[101]. CORREIA[102] vai mais longe ao entender estar consagrado um princípio mais amplo: o chamado «princípio da admissibilidade e equiparação dos contratos electrónicos aos contratos não electrónicos». Este mobiliza, por sua vez, a aplicação do princípio da liberdade contratual e do princípio da liberdade de forma, previstos nos artigos 405.º e 219.º do CC, respectivamente, posição que será por nós adoptada.

Pelo exposto, é natural que se conclua pela tendencial[103] validade destes contratos, atendendo, não apenas ao prescrito no artigo 12.º da Convenção (que trata sobre os contratos unilateral ou bilateralmente celebrados por meios automatizados), mas também pela remissão explícita para o "regime comum" prevista no n.º 1 do artigo 33.º da LCE, sendo por essa razão aplicável à contratação sem intervenção humana as normas do CC previstas nos artigos 217.º e seguintes, e outras normas que regulem a contratação através de meios electrónicos[104].

Antes de prosseguirmos, servem algumas notas sobre o aludido artigo 33.º da LCE: tendo a LCE sido destinada fundamentalmente a realizar a transposição da DCE, a norma em apreço constitui uma inovação do legislador português em relação àquela, ao regular a contratação sem intervenção humana, problemática não regulada pela Directiva[105]. Porém, considerando que interpretar a lei constitui uma tarefa que tem

101 Sobre o princípio da admissibilidade, cf., designadamente, J. ASCENSÃO (2003a), *op. cit.*, p. 241; Lei do Comércio Electrónico Anotada, *op. cit*., p. 96-98.
102 Cf. M. CORREIA (2013). 'Formação dos Contratos.' *AICEP*, p. 4. Obtido em 19 de Janeiro de 2018, disponível em http://www.aicep.pt/framework/download.php?id=98.
103 Cumpre-nos esclarecer que nem todos os contratos gozam desta protecção, ao terem sido expressamente excluídos pelo legislador (i) os negócios jurídicos familiares e sucessórios, (ii) os negócios jurídicos que exijam por lei a intervenção de tribunais, entidades públicas ou profissões que exercem poderes públicos, (iii) os negócios jurídicos de caução e garantias prestadas por pessoas agindo para fins exteriores à sua actividade comercial, empresarial ou profissional e (iv) os negócios jurídicos que criem ou transfiram direitos sobre bens imóveis, com excepção de direitos de arrendamento (cf. n.º 2 do artigo 25.º da LCE, e n.º 2 do artigo 9.º da DCE), sendo certo que estão fora do âmbito de aplicação da LCE (e da DCE) a matéria fiscal, a disciplina da concorrência, o regime do tratamento de dados pessoais e da protecção da privacidade, o patrocínio judiciário, os jogos de fortuna e azar em que é feita aposta em dinheiro, a actividade notarial ou equiparadas, nos termos do artigo 2.º da LCE (e no n.º 5 do artigo 1.º da DCE).
104 Cf. Lei do Comércio Electrónico Anotada, *op. cit.*, pp. 130-131.
105 Cf. A. L. PEREIRA (2004), *op. cit.*, §3.6 e J. ASCENSÃO (2003a), *op. cit.*, pp. 246-247.

como fim a descoberta do seu preciso e concreto sentido, e que se inicia a partir do seu elemento literal para se avaliar a *mens legislatoris*, devendo ser presumido que o «legislador consagrou as soluções mais acertadas e soube exprimir o seu pensamento em termos adequados»[106], cremos que o legislador foi infeliz ao incluir na redacção a parte final desta norma («salvo quando este pressupuser uma actuação»). Na verdade, o legislador quis dizer que à contratação celebrada exclusivamente por meio de computadores, sem intervenção humana, será aplicável o regime geral composto pelas normas do CC (artigos 217.º e seguintes) e por outras normas relativas à contratação através de meios electrónicos, e, nos casos em que para a conclusão de determinado contrato electrónico seja exigível intervenção humana, aplicar-se-á regime diverso[107], sem indicar, todavia, **qual** o regime então aplicável. Ora, não parece congruente que não seja aplicável o regime geral à contratação electrónica com intervenção humana, por força do princípio da especialidade, previsto no n.º 3 do artigo 7.º do CC. Aliás, por maioria de razão, apenas fará sentido que o regime geral seja aplicável a toda a contratação electrónica, salvo quando exista lei especial que derrogue a lei geral.

Destarte, tendo sido vontade do legislador apenas estender a aplicação do regime geral à contratação electrónica sem intervenção humana[108], a última parte da norma podia ser dispensada sem se perder o seu sentido[109]. Recorrendo às palavras de PINTO MONTEIRO, «deve o intérprete presumir que o legislador foi um *ás*, ainda que, porventura, na realidade, pudesse ter sido um *asno*!»[110].

Retomando o nosso percurso e julgando pela validade dos supramencionados contratos, estamos em condições de avançar para uma tentativa de enquadramento jurídico dos agentes de *software*. Anuindo com COELHO[111] e FESTAS[112], identificamos três enquadramentos potencialmente viáveis: (1) o *softbot* enquanto simples instrumento de transmissão da declaração, (2) o *softbot* enquanto núncio e (3) o *softbot* enquanto representante.

106 Cf. n.º 3 do artigo 9.º do Código Civil.
107 Cf. Lei do Comércio Electrónico Anotada, *op. cit.*, pp. 130-131.
108 Cf. J. ASCENSÃO, *in* ANACOM (2004), *op. cit.*, pp. 113-114; F. COELHO, *op. cit.*.
109 No mesmo sentido, cf. A, MARTINS, J. MARQUES & P. DIAS (2012). *Cyber Law in Portugal*, p. 193.
110 Cf. A. Pinto MONTEIRO (2017). 'A cláusula penal perante as alterações de 1980 e de 1983 ao Código Civil.' *Revista de Legislação e de Jurisprudência* (GESTLEGAL) 4006, p. 9.
111 Cf. F. COELHO, *op. cit*..
112 Cf. D. FESTAS, *op. cit*., pp. 419-425.

Vejamos:

(1) O *softbot* enquanto simples instrumento de transmissão de declaração[113]

Considerando o que já foi explicitado sobre o funcionamento dos *softbots*, torna-se evidente a inaplicabilidade deste enquadramento, atenta a capacidade de autonomia decisória do *softbot*. É claro que o agente executa a sua programação de maneira a atingir o fim a que foi destinado; porém, todo o processo de contratar (preparar, negociar e contratar) cabe exclusivamente àquele. Assim, de uma instrução incompleta, mas adequada, nasce um contrato que talvez não tivesse sido sequer cogitado pelo sujeito utilizador. É esta distância que se verifica entre as instruções do sujeito utilizador e do contrato-resultado que nos permite dizer que o *softbot* não é um simples instrumento.

(2) O *softbot* enquanto núncio[114]

Como é do conhecimento geral, o núncio figura somente como um *longamanus*, limitando-se a transmitir apenas a declaração de outrem[115]; como se acabou de ver, a instrução incompleta, mas adequada, do sujeito utilizador, não se identifica com o contrato celebrado pelo *softbot*, pelo que também este enquadramento não nos parece configurável.

(3) O *softbot* enquanto representante[116]

Prevista no artigo 258.º do CC, a representação consiste na prática de certo acto jurídico em nome de outrem, tendo em vista a produção dos respectivos efeitos jurídicos na esfera dessa outra pessoa[117]. Este acto é eficaz, mesmo que não seja concluído no interesse do representado, mas desde que o representante não exceda os «limites dos poderes que lhe competem» (artigo 258.º do CC). Ora, na contratação electrónica com recurso a *softbots*, como já se disse, o sujeito utilizador dirige ao *softbot* uma instrução incompleta, mas adequada, sendo função do *softbot* interpretar a 'vontade' daquele, para melhor cumprir autonomamente a sua finalidade, adaptando e modificando a sua

113 Cf. F. COELHO, *op. cit.*.
114 *Idem, ibidem.*
115 Cf. C. Mota PINTO (2005). *Teoria Geral do Direito Civil.* 4ª edição, pp. 543-544; A. Menezes CORDEIRO (2017b). *Tratado de Direito Civil*. Vol. V, p. 120.
116 Cf. F. COELHO, *op. cit.*.
117 Cf. C. Mota PINTO, *op. cit.*, pp. 539-547.

actuação em conformidade com as eventuais informações que for recebendo/captando do mundo físico e/ou digital.

Como se demonstrou, o agente não se limita a transmistir a declaração negocial do seu sujeito utilizador; aliás, ousamos dizer que o agente é portador de uma espécie de 'vontade' que é 'sua', possibilitando-lhe a faculdade de produzir e emitir uma declaração negocial. Desta forma, torna-se possível um contrato: de um lado temos o *softbot* responsável pela compra da caneta ∂, ao *melhor preço*[118] e, do outro, teremos um segundo *softbot*, este responsável pela venda de canetas ∂, da melhor qualidade, ao preço mais baixo, na plataforma TauBuy. Em suma, parece-nos que a representação configura o melhor enquadramento para as competências do agente de *software*[119].

Ainda que se aceite este terceiro enquadramento como possível e justificável, duas questões ficam por resolver[120]:

(1) Visto que o agente de *software* não tem, à partida, personalidade jurídica, será aquele enquadramento *compatível*?

(2) Considerando que o agente não se figuraria nem como o nosso típico representante, nem seria emissor de declarações negociais iguais às emitidas por um humano, *em que medida seriam os respectivos regimes aplicáveis*?

Debruçando-nos sobre a primeira questão colocada, *prima facie*, parece que o enquadramento que fizemos seria incompatível, já que o agente de *software* seria um representante sem personalidade jurídica. Porém, entendemos não ser completamente inconcebível[121], por estar previsto no artigo 263.º do CC que «[o] procurador não necessita de ter mais do que a capacidade de entender e querer»[122], e já demonstrámos que o nosso agente de *software* detém esta competência.

Adicionalmente, ainda que o legislador não tenha expressamente exigido que o representante fosse uma entidade portadora de personalidade jurídica (*rectius* um humano), no limite parece pressupor tal exigência, em virtude do facto do ser humano

118 Recorde-se o exemplo apresentado *supra* §4.2 Caracterização dos agentes de *software.*
119 No mesmo sentido, cf. D. FESTAS, *op. cit.*, pp. 419-425; F. COELHO, *op. cit.*.
120 As mesmas questões são colocadas por F. COELHO, *op. cit.*.
121 No mesmo sentido, cf. F. COELHO, *op. cit.*
122 Cf. A. Menezes CORDEIRO (2017b), *op. cit.*, pp. 123-124.

ser (ter sido) o único dotado daquelas capacidades – que por sua vez lhe permitiriam agir em nome de outrem. Mas também já vimos que o agente de *software* é dotado de capacidades de cognição e volição, pelo que nada parece obstar a uma interpretação actualista desta exigência aparentemente implícita. Diremos que não parecer obstar, pois o nosso ordenamento jurídico já atribui personalidade jurídica às pessoas colectivas (que se trata de «um processo técnico de organização das relações jurídicas conexionadas com um dado empreendimento colectivo»[123]), que podem ser constituídas por um conjunto de pessoas ou por uma massa de bens, não existindo necessariamente uma personalidade *humana* e não lhes sendo negado o direito de representar outrem[124].

Além disso, ainda que não seja admissível tal interpretação à luz do direito constituído, uma alteração legislativa poderia facilmente resolver a incompatibilidade, passando a reconhecer uma capacidade de agir limitada às capacidades de actuação do *software*, que não assentasse numa personalidade jurídica. Esta opção não seria novidade no direito comparado[125], atenta a proposta de revisão do *Uniform Commercial Code* da *National Conference of Commissioners on Uniform State Laws* e da *American Law Institute* em 1996[126].

Sendo assim, respondendo à primeira questão que colocámos, entendemos ser tal enquadramento compatível, ainda que ao agente de *software* não seja atribuída personalidade jurídica, posto que é o próprio legislador que é omisso quanto à (in)exibilidade desta, sendo bastante as capacidades de compreender, querer e agir.

Relativamente à segunda questão colocada, importa desde já clarificar que, sendo o recurso ao regime da representação justificado e possível, este será, em princípio,

123 Cf. A. Mota PINTO, *op. cit.*, pp. 193-94 e 269.
124 Cf., nomeadamente, P. CUNHA (1985). 'As pessoas colectivas como administradores de sociedades.' *Revista da Ordem dos Advogados* I (45), pp. 5-11; T. SANTOS (2014). 'A Designação de Pessoas Colectivas para o Órgão de Administração de Sociedades Comerciais.' *Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Empresariais/Menção em Direito Empresarial*, pp. 78-80.
125 Cf. J. DODD & J. HERNANDEZ (1998). 'Contracting In Cyberspace.' *Computer Law Review and Technology Journal* (Summer), p. 4; J. FISCHER, *op. cit.*, pp. 556-564.
126 Esta proposta de revisão procurava modernizar o Artigo 2.º, relativo à venda de bens, introduzindo o conceito de *electronic agency*. Porém, dada a falta de adopção pelos diversos Estados, aquelas instituições abandonaram a proposta, não tendo sido aprovada a revisão. Sobre esta revisão, cf. Uniform Commercial Code Article 2B: Licences (DRAFT), de 25 de Julho - 1 de Agosto de 1997. Disponível em http://www.uniformlaws.org/shared/docs/computer_information_transactions/2b/ucc2bam97.pdf (Obtido em: 27 de Janeiro de 2018); B. BLUM & A. BUSHAW (2017). *Contracts: Cases, Discussion and Problems.* Wolters Kluwer Law & Business. §3. Revisions of the UCC; J. FISCHER, *op. cit.*, pp. 556-564.

também *necessário*[127], na medida em que o agente de *software* não é apenas um instrumento do seu sujeito utilizador, mesmo que não dotado de personalidade jurídica. Desta maneira, a representação parece ser o instituto ideal para acautelar os interesses das partes: por um lado, a possibilidade do sujeito utilizador se poder escudar das decisões que sejam contrárias às instruções originais assumidas pelo seu agente de *software*; e, por outro, da contraparte que confiou no contrato que celebrou com o *softbot*, devendo estes contratos ser, em regra, válidos.

Não sendo sempre possível prever as decisões que o *softbot* tomará para completar a instrução incompleta, mas adequada, que lhe é dada, não poderia ser exigido do sujeito utilizador a manifestação antecipada da sua efectiva vontade de celebrar determinado negócio jurídico futuro cujo conteúdo ainda é desconhecido, sob pena de se constituir um vício de falta de consciência da declaração (artigo 246.º CC)[128]. Além disso, também não se poderia conceber um sistema de confirmação póstuma (tanto no caso de se aceitar referida hipótese de manifestação antecipada, no sentido de se sanar o aludido vício, nos termos do artigo 288.º do CC, como no caso de se aceitar a existência de uma «condição suspensiva de perfeição do contrato»[129])[130], porquanto contrariar-se-ia o sentido da contratação automatizada, não sendo por isso eficiente[131]. Como tal, é o instituto da representação que permite a produção dos efeitos do negócio jurídico celebrado pelo representante (o agente de *software*) em nome do representado (o sujeito utilizador)[132] na esfera jurídica deste, porquanto a actuação representativa, além de significar que o representante actua juridicamente em nome do representado e que não é autor do acto, também significa que aquele não pretende que os efeitos do referido negócio se façam sentir na sua esfera jurídica[133].

Ademais, é também o regime da representação que permite ao representado desvincular-se de determinado negócio que tenha sido celebrado pelo representante quando este viole as instruções que lhe foram inicialmente dadas, abusando dos poderes

127 Cf. F. COELHO, *op. cit.*.
128 Cf. A. Menezes CORDEIRO (2017a), *Tratado de Direito Civil*. Vol. II, pp. 787-797.
129 Cf. A. L. PEREIRA (2004*), op. cit.*, pp. 346-348.
130 Cf. M. BARBOSA (2017). 'Erro na formação do negócio jurídico e contratação eletrónica.' *Boletim da Faculdade de Direito* I (XCIII), pp. 185-186.
131 No mesmo sentido, F. COELHO, *op. cit.*.
132 Dispõe o artigo 258.º do Código Civil que «[o] negócio jurídico realizado pelo representante em nome do representado, nos limites dos poderes que lhe competem, produz os seus efeitos na esfera jurídica deste último».
133 Cf. A. PRATA (2017). *Código Civil Anotado*. Vol. I, pp. 311-312 (§7).

de representação[134], ou agindo como um «representante sem poderes ou '*falsus procurator*'»[135]. Faculdade esta que não seria tão fácil de aceder se aceitássemos os enquadramentos do agente de *software* enquanto instrumento ou do agente de *software* como núncio, ao exigir-se a verificação do erro na transmissão da declaração do representado ou da relevância do seu erro mecânico[136].

Concordámos com COELHO[137] quando indicámos que o enquadramento do agente de *software* enquanto representante seria possível, justificado e, em princípio, necessário. Todavia, algumas notas devem ser tidas em conta antes de considerarmos que o enquadramento é efectivamente necessário, sob pena de irreflectidamente pressupormos que todo o regime jurídico (ou grande parte deste) seria analogicamente aplicável aos agentes de *software*. Questão que iremos ver já de seguida.

5.4 O (eventual) regime jurídico dos agentes de *software*

Se, por um lado, encontramos a posição de COELHO[138] que defende que a caracterização dos agentes de *software* poderia ser compatibilizada (mediante certas adaptações) com o instituto da representação, por outro, encontramos a Resolução do Parlamento Europeu de 16 de Fevereiro de 2017[139] (que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica), em que se invoca a necessidade da criação de um regime próprio para estes[140_141].

134 Cf. A. Mota PINTO, *op. cit.*, p. 550; A. Menezes CORDEIRO (2017b), *op. cit.*, pp. 153-154.; L. FERNANDES (2010). *Teoria Geral do Direito Civil.* Vol. II, pp. 274-275; artigo 269.º CC.
135 Cf. A. Mota PINTO, *op. cit.*, p. 549; A. Menezes CORDEIRO (2017b), *op. cit.*, pp. 150-152; L. FERNANDES, *op. cit.*, pp. 271-274; artigo 268.º CC.
136 Cf. F. COELHO, *op. cit.*.
137 Cf. *Idem, ibidem.*
138 Cf. *Idem, ibidem.*
139 Doravante 'Resolução'. Disponível em http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//PT (obtido em 28 de Janeiro de 2018).
140 Lê-se naquele: Considerando que «as máquinas concebidas para escolher as suas contrapartes, para negociar as condições contratuais, para celebrar contratos e para decidir se e como os aplicam, invalidam a aplicação das normas tradicionais; considerando que isto sublinha a necessidade de novas normas, eficientes e mais atualizadas».
141 Acrescente-se que, além do Parlamento Europeu, também outras entidades adoptaram esta opinião – v., por exemplo, o discurso de R. THOMAS (2017). "'Law Reform Now' in 21st Century Britain: Brexit and Beyond." *6th Scarman Lecture.* Gray's Inn (§39), juiz Britâncio e ex-*Lord Chief Justice of England and Wales*, que frisa a importância de uma actualização legislativa – ou, tendo ido mais longe, propondo uma alteração, como é o caso do Estado de Florida dos EUA, com a sua *House Bill* 1357, nas suas linhas 48 a 54, proposta a 26 de Janeiro de

De facto, a adopção de um regime próprio *de jure constituendo* seria deveras vantajosa, ao permitir, em princípio, a previsão de diversas soluções que, com grande certeza, não iremos encontrar se nos limitarmos a uma aplicação analógica do aludido regime comum. Porém, também não nos parece irrazoável optar por uma alteração legislativa, de maneira a contemplar determinadas soluções que as normas tradicionais não prevêem[142].

De uma maneira ou de outra, a verdade é que o nosso legislador já em 2004 previu, na LCE, a contratação sem intervenção humana[143], à qual remete a aplicação do regime geral[144]. Tendo em conta tudo o que foi aqui mencionado anteriormente, não choca que concordemos novamente com COELHO[145], ao afirmarmos que, caso se legisle *ex novo*, esse regime muito provavelmente se aproximará do regime geral da representação e da declaração negocial. Por conseguinte, importa desde logo tratar de três questões: a 'procuração' do agente de *software*, a forma e o momento da celebração do contrato, e o 'erro' do agente de *software*. Vejamos:

5.4.1 A 'procuração' do agente de *software*

A procuração trata-se do acto unilateral pelo qual certa pessoa atribui poderes representativos a outrem (cf. artigo 262.º do CC)[146]. No caso do agente de *software*, este acto teria de ser traduzido em algum comportamento que compreendesse a concessão voluntária de poderes representativos, mesmo que este fosse apenas tacitamente compreendido como tal (v.g. o acto de programar o agente de *software*).

5.4.2 A forma e o momento de celebração do contrato

Como se sabe, vigora no ordenamento jurídico português o princípio da autonomia privada, que consiste no reconhecimento do poder de autorregulamento dos

2018, estando disponível *online* em: https://legiscan.com/FL/text/H1357/id/1676376/Florida-2018-H1357-Introduced.pdf (Obtido em 28 de Janeiro de 2017).

142 A. Menezes CORDEIRO (2017a, *op. cit.*, p. 355), reconhecendo a natureza civil das disposições relativas à contratação electrónica sem intervenção humana previstas na LCE, adverte que apenas será recomendável qualquer «mexidas na lei civil» após uma cuidada preparação, ainda que se pudesse obter maior clareza mediante uma «codificação condigna, na lei civil geral».

143 Cf. artigo 33.º da LCE.

144 V. supra §4.3 A qualificação jurídica dos agentes de *software*.

145 Cf. F. COELHO, *op. cit.*

146 Cf., entre outros, A. Mota PINTO, *op. cit.*, pp. 541-542; A. PRATA, *op. cit.*, pp. 318 *et seq.*; L. FERNANDES, *op. cit.*, pp. 267-270; A. Menezes CORDEIRO (2017b), *op. cit.*, pp. 128-132.

interesses dos particulares e de autogoverno da sua esfera jurídica (cf. artigo 405.º do CC), sendo a liberdade contratual e a liberdade de forma, (cf. artigo 219.º do CC) as suas mais notórias manifestações.

Remetendo para o que já foi referido quanto ao princípio da admissibilidade e equiparação dos contratos electrónicos aos contratos não electrónicos[147], importa recordar que a contratação electrónica pode ser equiparada à contratação 'tradicional' na medida em que recorre ao uso de *software/hardware* para produzir a declaração negocial, a meios de transporte de dados para transmitir a referida declaração, e à assinatura electrónica qualificada ou digital para que passem a funcionar as presunções de autoria, vontade e inalterabilidade, previstas nas alíneas a) a c) do n.º 1 do artigo 7.º do RJDEAD[148].

No entender de COSTA[149], encontramos dois casos de sobreposição de normas: no primeiro caso, encontramos as normas do RJDEAD (cf. n.º 1 do artigo 1.º e n.º 1 do artigo 3.º) que vêm dizer que aquele diploma regula a validade, eficácia e valor probatório dos documentos electrónicos, e que os documentos electrónicos satisfazem o requisito legal de forma escrita, quando o seu conteúdo seja susceptível de representação como declaração escrita, o que contrasta com o disposto na LCE (cf. n.º 1 do artigo 25.º), onde é consagrado o aludido princípio da admissibilidade e equiparação dos contratos electrónicos aos contratos não electrónicos. No segundo, deparamo-nos com o texto do n.º 1 do artigo 3.º do RJDEAD (que prevê a satisfação do requisito legal de forma escrita dos documentos electrónicos quando o seu conteúdo seja susceptível de representação como declaração escrita, como se acabou de ver), que parece confrontar o prescrito no n.º 1 do artigo 26.º da LCE (que estatui que as declarações emitidas por via electrónica satisfazem o requisito legal de forma escrita quando contidas em suporte que ofereça as mesmas garantias de fidedignidade, inteligibilidade e conservação).

É evidente que em ambos os casos a LCE vai mais longe, evidenciando-se a equiparação dos contratos electrónicos aos contratos não electrónicos, mas não entendemos que estas sobreposições invalidem o relevo do disposto no n.º 1 do artigo

147 V. supra §4.3 Qualificação jurídica dos agentes de *software*.
148 V. supra §2. A assinatura electrónica.
149 Cf. P. Costa e SILVA (2005), *in* Lei do Comércio Electrónico Anotada, *op. cit.*, pp. 183-185.

3.º do RJDEAD, na medida que é a partir desta norma que se viabiliza a aplicação das regras relativas à prova documental.

Considerando que o agente de *software* possui capacidades cognitivas e volitivas, que o sujeito utilizador, por acto unilateral, confere ao *softbot* poderes representativos e que, por via das suas capacidades, o agente é capaz de agir 'em nome' do sujeito utilizador, diremos que a forma electrónica da 'vontade' do *softbot* e da emissão e recepção da declaração dessa 'vontade' não chocará com as disposições que acabámos de referir, uma vez que todos os intervenientes (i.e. os sujeitos utilizadores e os *softbots* que intervenham no negócio jurídico) possuem a sua própria assinatura electrónica, o que irá permitir a identificação de todos os actos electrónicos praticados pelos intervenientes (visto que todos os actos são inscritos na plataforma e, por isso, assinados electronicamente[150]). Além disso, ainda que os *softbots*, na interacção que (eventualmente) façam com outros agentes de *software*, o façam numa linguagem 'própria', pode (e deve) esta linguagem ser traduzida – ou traduzível – para uma linguagem humana, passando a ser susceptível de representação escrita, viabilizando, como se disse, a aplicação das regras relativas à prova documental.

Por fim, algumas notas relativamente ao momento da celebração do contrato: na formação do contrato identificam-se (pelo menos) duas declarações negociais: a proposta e a aceitação, que se devem conciliar num consenso. Aqui chegados, coloca-se o problema em saber qual o momento da sua perfeição. Sendo várias as doutrinas que tentam apresentar uma solução para este problema, foi adoptado pelo legislador de 1966 (e também pelo legislador alemão e pela Convenção de Viena sobre compra e venda internacional de mercadorias), no artigo 224.º do CC, a doutrina da recepção, que defende que «o contrato está perfeito quando a resposta contendo a aceitação chega[r] à esfera de acção do proponente»[151].

Assim, no contexto da forma de contratação electrónica automatizada que temos analisado, visto que todos os actos electrónicos levados a cabo pelos intervenientes, humanos ou não (v.g. inscrição do *smart contract*/agente de *software* na plataforma e das instruções iniciais, análise (por parte do agente) dos dados disponíveis relevantes para a tomada de decisão, negociação do conteúdo do contrato, emissão da declaração

150 Cf. Figuras 1, 2 e 3.
151 Cf. A. Mota PINTO, *op. cit.*, pp. 648-650.

negocial, etc.), são inscritos e assinados electronicamente na plataforma, dir-se-á que o momento da perfeição negocial será atingido quando se verifique a validade e legitimidade para negociar e seja atingido um consenso entre as duas declarações negociais, que por sua vez resultará numa operação *output*. Como tal, poderão a data e hora da criação, expedição ou recepção dos actos electrónicos ser identificados pela análise da informação contida na assinatura electrónica[152].

5.4.3 O 'erro' do agente de *software*

Já vimos que o agente de *software* é uma entidade dotada de autonomia e de (limitada) *inteligência*, no entanto, não deixa de ser um produto da criatividade e dos avanços tecnológicos humanos, pelo que seria inconcebível afirmar que estes estariam imunes ao erro (ainda que estes estivessem munidos de uma excepcional capacidade de auto-aprendizagem e/ou de adaptação). O funcionamento do agente de *software* consiste, essencialmente, na execução do seu código fonte e das instruções iniciais programadas pelo seu sujeito utilizador, sendo possível que o seu código fonte e/ou a programação inicial do sujeito utilizador conheça falhas ou vícios. Dito por outras palavras: é possível que algum erro na execução do código fonte do agente de *software* ocorra independentemente do facto de as instruções inicias terem sido correctamente inseridas e compreendidas pelo agente.

Avançámos *supra* a possibilidade de o agente agir sem poderes ou em abuso de representação[153]; se uma situação destas ocorresse num contexto de contratação 'tradicional', os interesses do representado estariam salvaguardados na medida em que o negócio celebrado nessas condições seria ineficaz em relação a ele, nos termos do n.º 1 do artigo 268.º do CC. Porém, o nosso agente não é uma entidade dotada de personalidade jurídica e também não dispõe de um património responsável para poder responder por eventuais danos que cause à contraparte, o que parece levantar um problema.

152 V. *supra* §2. A assinatura electrónica.
153 Cf. A. Mota PINTO, *op. cit.*, pp. 549-550; A. Menezes CORDEIRO (2017b), *op. cit.*, pp. 150-154.; L. FERNANDES, *op. cit.*, pp. 271-275.

COELHO[154] resolve esta questão ao convocar a aplicação (com as devidas adaptações) do regime da representação aparente do contrato de agência, previsto no artigo 23.º do DL n.º 178/86, de 3 de Julho, alterado pelo DL n.º 118/93, de 13 de Abril[155–156], justificando que também esta relação existente entre o sujeito utilizador e o seu agente de *software* constituirá uma espécie de relação de cooperação, admitindo-se assim a extensão daquela norma a este regime. Porém, esta solução não resolve o problema do erro humano na programação do agente, nem do funcionamento deficiente do *software*.

O Código Civil, prevendo o erro como causa de invalidade do negócio jurídico, reparte-o em duas modalidades: o erro-obstáculo (ou erro na declaração) e o erro-vício. Enquanto o primeiro é tido como uma «divergência não intencional entre a vontade e a declaração»[157], o segundo prevê que a vontade se formou de modo deficiente, consubstanciando um vício na formação da vontade[158].

É verdade que o nosso legislador apresentou uma solução para estes problemas nas alíneas a) a c) do n.º 2 do artigo 33.º da LCE[159], mas entendemos que a simples aplicação analógica daquele regime poderá resultar em soluções menos acertadas[160]. Vejamos as três categorias de erro, considerando, a título de exemplo, as seguintes situações:

(i) O erro de programação

Hipótese 1:

António programa o seu *softbot* para adquirir a obra *1986*, convencido de que o autor da mesma é George Orwell e de que se trata de ficção científica. Na verdade, o autor da obra *1986* é Morgan Parker e trata-se de um *thriller*. *Quid iuris?*

154 Cf. F. COELHO, *op. cit.*.
155 Dispõe o n.º 1 do artigo 23.º do Diploma: «O negócio celebrado por um agente sem poderes de representação é eficaz perante o principal se tiverem existido razões ponderosas, objectivamente apreciadas, [...]».
156 Cf. A Pinto MONTEIRO (2017). 'Revisitando a Lei da Agência 30 anos depois.' *Distribuição comercial nos 30 anos da Lei do Contrato de Agência*, pp. 58 e 78-80.
157 Cf. A. Pinto MONTEIRO (2004). 'Erro e teoria da imprevisão.' *Estudos de Direito do Consumidor* (6), p. 324.
158 Cf. A. Menezes CORDEIRO (2017a), *op. cit.*, pp. 848- 874; M. BARBOSA, *op. cit.*, pp. 187-188.
159 Assim, havendo erro na programação, aplicar-se-ia o regime do erro da formação da vontade (alínea a)), havendo funcionamento defeituoso, aplicar-se-ia o regime do erro na declaração (alínea b)) e havendo defeito na mensagem aquando da sua recepção pelo destinatário, aplicar-se-ia o regime do erro na transmissão (alínea c)).
160 Cf. M. BARBOSA, *op. cit.*, pp. 186-187.

Hipótese 2:

Bernardo, leitor ávido e amante de ficção científica, em conversa com a sua amiga **Camila**, teve conhecimento do lançamento de uma edição exclusiva do seu livro preferido de Douglas Adams – *The Hitchhiker's Guide to the Galaxy* – assinada pelo autor. Interessado em adquirir uma cópia, mas não sabendo onde comprar, instrui o seu ***softbot*** a procurar e comprar uma cópia. Por engano, **Bernardo**, no momento em que introduzia o valor da quantidade de exemplares a adquirir, acrescenta um zero a mais, resultando numa instrução de aquisição de dez exemplares do livro em vez de apenas um. *Quid iuris?*

Na primeira hipótese representa-se uma situação em que o sujeito utilizador programa correctamente o seu agente de *software* e este segue rigorosamente as instruções. Todavia, a vontade que esteve na base da programação está viciada por erro-vício, na medida em que **António** está em erro sobre as qualidades essenciais do objecto, enquanto falsa representação das circunstâncias em que se fundou a decisão de contratar, já que o autor é na realidade Morgan Parker, e não se trata de uma ficção científica, mas antes de um *thriller*.

Já na segunda, figura-se uma situação em que não existe um erro-vício, como se passava na primeira hipótese, mas também não existe um erro-obstáculo, visto que, se o processo de programação se assemelha a um «processo volitivo interno»[161] e se a emissão da declaração automatizada só irá ser formulada posteriormente pelo *softbot*, inexiste uma divergência entre a vontade expressa por **Bernardo** e a declaração negocial, já que esta ainda não foi emitida pelo agente de *software*.

Em ambas as hipóteses, deparamo-nos com erros de programação, que, por remissão do disposto na alínea a) do n.º 2 do artigo 33º da LCE, nos levaria à aplicação das regras previstas no artigo 251.º (erro-vício sobre o objeto do negócio ou sobre a pessoa do declaratário), nos n.º 1 (erro-vício sobre os motivos) e n.º 2 (erro-vício sobre a base do negócio) do artigo 252.º, todos do CC. Assim, para a *primeira hipótese*,

161 Cf. D. FESTAS, *op. cit*., p. 440.

convocar-se-ia a aplicação do disposto no artigo 247.º *ex vi* o artigo 251.º, por se tratar de uma situação que se aproxima de um erro-vício sobre o objecto.

Atento o que fora dito sobre o tipo de erro presente na <u>*segunda hipótese*</u>, que regime seria, então, aplicável? Por falta de compatibilidade, entendemos que nenhuma das regras poderia ser convocada, embora concordemos com a solução apresentada por FESTAS, que propõe a aplicação do artigo 247.º do CC, «não apenas pela analogia existente com as situações tradicionais de erro na declaração, como também pelo facto de [...] todo o processo de preparação e programação [...] dever ser equiparado ao processo volitivo interno de formação da vontade que se verifica na contratação comum»[162]. Mesmo assim, o recurso a este regime conduzir-nos-á a outra dificuldade: a de inserir no código fonte do agente de *software* a capacidade de conhecer, ou não poder ignorar, a essencialidade do elemento sobre que incidiu o erro, pelo que, não sendo isso possível e adoptando a posição de diversos autores[163], teríamos de aplicar os requisitos constantes no artigo 247.º do CC aos sujeitos utilizadores[164], porquanto são estes os sujeitos que verdadeiramente celebram o contrato, ainda que por intermédio do(s) seu(s) *softbot(s)*.

(ii) O funcionamento defeituoso do agente de *software*

<u>*Hipótese 3:*</u>

Dulce, após recorrentes insistências do seu amigo **Evaristo**, ambos entusiastas de filmes de ficção científica, instrui o seu ***softbot*** a adquirir o primeiro filme da saga *Guerra das Estrelas*, para que pudesse assistir <u>como um verdadeiro fã</u>. Momentos mais tarde, após indicação do cumprimento da instrução dada, **Dulce** e **Evaristo** são surpreendidos ao verificar que, ao invés de ter sido adquirido o *Episódio IV – Uma Nova*

162 Cf. *Idem, ibidem*, pp. 445-446 (nota 82).
163 Neste sentido, cf. D. FESTAS, *op. cit.*, pp. 444-446; V. ROSA (2005) *in* Lei do Comércio Electrónica Anotada, *op. cit.*, p. 205; J. ASCENSÃO (2003b). 'Contratação electrónica.' *Direito da Sociedade da Informação*, Vol. IV, p. 67.
164 Invocando, por exemplo e como propõe J. ASCENSÃO (2003b, *op. cit.*, *loc. cit.*), «a culpa *in contrahendo*», «o risco» ou «a teoria da aparência».

Esperança, de 1977, como era expectável, foi adquirido o *Episódio I – A Ameaça Fantasma*, de 1999. *Quid iuris?*

Nesta situação, o vício não advém de uma actuação humana e tem como resultado uma divergência não intencional entre a programação (e a vontade aí expressa) e a declaração emitida pelo *softbot.* Assim, considerando o disposto na alínea b) do n.º 2 do artigo 33.º e no n.º 3 do artigo 33.º, ambos da LCE, deveria ser aplicada a regra do artigo 247.º do CC, devendo, por essa ordem de razão, provar-se a essencialidade do elemento sobre que incidiu o erro. Porém, nem por isso seria esta solução ajustada. O facto de se ter verificado uma divergência entre a vontade que o sujeito utilizador pretendia que fosse exteriorizada e a vontade que foi exteriorizada pelo *softbot* (ao invés de uma divergência entre a vontade que o sujeito utilizador queria exprimir e que efectivamente exprimiu na programação (como vimos anteriormente)) não afasta o problema que encontrámos na tentativa de solução da *segunda hipótese*.

(iii) O erro na transmissão da mensagem aquando da sua recepção pelo destinatário

Hipótese 4:

Fátima, guia turística por profissão**,** tendo tido conhecimento que iria ser realizada uma exposição interactiva em Londres para celebrar os 55 anos da sua série televisiva britânica de ficção científica preferida, *Doctor Who*, instrui o seu ***softbot*** a negociar e adquirir um pacote de viagem que contemple a passagem de avião e a estadia num hotel próximo da exposição. Mas, no decurso da transmissão da mensagem (*rectius* da execução da instrução), a declaração deforma-se e, no lugar de adquirir um pacote de viagem para uma pessoa, é adquirido um pacote para um grupo de 10 pessoas. *Quid iuris?*

Situação mais difícil de conceber, dado o modo de funcionamento das DLT, é a identificação de uma deformação na mensagem durante a sua transmissão sem se confundir com um funcionamento defeituoso do agente de *software.* FESTAS, na tentativa de apresentar uma solução para uma hipótese semelhante à nossa, refere ser imprescindível identificar se a transmissão da mensagem é feita por via de um servidor

do declarante ou por via de um servidor intermediário, pois concorrem fundamentos diferentes para a mesma solução: a vinculação do declarante[165]. Ora, na nossa situação, é preciso recordar que uma plataforma fundada em DLT será necessariamente descentralizada, sendo todos os actos verificados e registados por todos os nodos da rede, sendo desde logo muito difícil cogitar uma tal situação de erro de transmissão[166]. Por essa razão, das duas, uma: ou estaremos perante um erro de funcionamento de (pelo menos) um agente de *software* dos vários nodos da rede, responsáveis pela verificação e inscrição e dos actos no livro-razão dos nodos, ou estaremos perante uma operação *fork*, que veio permitir a inscrição e execução de um acto electrónico que era anteriormente impossível[167].

De uma maneira ou de outra, tendo em vista todas as hipóteses que apresentámos, e sem desconsiderar o iter percorrido por FESTAS[168] quanto ao regime aplicável ao erro de programação, ao erro na declaração e ao erro na transmissão na contratação electrónica automatizada, entendemos que o actual regime comum aplicável a estas situações carece de uma reforma, visto que, na altura da sua concepção, não se havia cogitado uma realidade como a nossa: um agente não humano, com capacidades cognitivas e volitivas, capaz de agir 'em nome' de outrem, mas que carece de personalidade jurídica. Em suma, os problemas com que somos confrontados resultam de uma tentativa de aprisionamento de possíveis problemas jurídicos em quadros conceptuais estanques, tendo sido preferível que o legislador se tivesse limitado a dispor que a disciplina do erro é aplicável à contratação sem intervenção humana[169].

A Resolução, ciente dos problemas levantados pela impossibilidade de responsabilização dos robôs pelas suas acções ou omissões quando não seja possível

165 Sumariamente, o autor entende que haverá sempre vinculação do declarante mas por fundamentos diversos: no caso de se tratar de um servidor do declarante, haverá vinculação do declarante, na medida em que o servidor equiparar-se-á a um núncio, por força de uma relação contratual entre o declarante e o servidor; no caso de se tratar de um servidor intermediário, haverá vinculação pelo facto de ter sido o declarante que escolheu aquele meio de transmissão, devendo por isso suportar o risco, aplicando-se a aplicação analógica do artigo 250.º do Código Civil – v. D. FESTAS, *op. cit.*, pp. 456-460.

166 Aliás, se assim fosse, que segurança traria esta tecnologia que se gaba pela renúncia de terceiros intermediários? Veja-se que no *blockchain* da *bitcoin*, é exatamente no processo de verificação que se impede que seja transferida uma quantia superior à soma disponível na carteira electrónica; se é assim, no nosso exemplo, o pedido corresponderia à 'soma disponível' do exemplo antetior da *bitcoin* e a declaração a ser emitida pelo *softbot* a 'quantia a transferir'. Em suma, esta tecnologia gaba-se pela impossibilidade de *double spending*.

167 Assim, por exemplo, passaria a ser possível 'autorizar' a transferência de 10 *bitcoins* da conta A para a conta B quando na conta A existiam somente 5 *bitcoins.*

168 Cf. D. FESTAS, *op. cit.*, pp. 433-460.

169 Cf. M. BARBOSA, *op. cit.*, p. 202; D. FESTAS, *op. cit.*, p. 444.

atribuir a causa a um interveniente humano, prescreve que não deverão, de modo algum, «limitar[-se] o tipo ou a extensão dos danos a indemnizar nem as formas de compensação que podem ser disponibilizados à parte lesada, pelo simples facto de os danos terem sido provocados por um agente não humano», evidenciando-se, também aqui, um corolário de não discriminação em razão do sujeito[170].

6. ALGUMAS NOTAS SOBRE A RESOLUÇÃO DO PARLAMENTO EUROPEU

As patentes dificuldades que acabámos de expor no capítulo anterior, na tentativa de enquadrar um regime jurídico aplicável aos agentes de *software* são, de certo modo, espelhadas na Resolução do Parlamento Europeu, de 16 de Fevereiro de 2017, que teve como desiderato apresentar à Comissão e ao Conselho algumas recomendações quanto às disposições de Direito Civil sobre Robótica[171].

Eis que, à semelhança da dificuldade em codificar a capacidade de conhecer, ou não poder ignorar, a essencialidade do elemento sobre que incidiu o erro que vimos *supra*[172], vem a Resolução afirmar que as Leis de Asimov[173] devem ser encaradas como dirigidas «aos criadores, aos produtores e aos operadores de robôs, incluindo robôs com autonomia integrada e autoaprendizagem», apoiando-se precisamente na dificuldade em traduzir e incorporar estas regras no código fonte do *software*[174].

170 Cf. Considerando (52) da Resolução.
171 Versando sobre, nomeadamente, os princípios gerais, a responsabilidade, os princípios gerais relativos ao desenvolvimento da robótica e da inteligência artificial para utilização civil, os princípios éticos, a normalização, segurança e protecção e as licenças para os criadores e utilizadores de robôs.
172 V. *supra* §4.4.3 O erro do agente de *software*.
173 ASIMOV definiu as Três Leis da Robótica como: (1) um robô não pode magoar um ser humano ou, por inação, permitir que tal aconteça; (2) um robô tem de obedecer às ordens dos seres humanos, excepto se essas ordens entrarem em conflito com a primeira lei; (3) um robô tem de proteger a sua própria existência desde que essa proteção não entre em conflito com a primeira ou com a segunda lei; e, mais tarde, (0) um robô não pode magoar a humanidade ou, por inação, permitir que a humanidade se magoe. Cf. I. ASIMOV (1943). "Runaround." *I, Robot*, pp. 27 *et seq.* Obtido em 30 de Janeiro de 2018, disponível em http://kaitnieks.com/files/asimov_isaac__i_robot.pdf.
174 Cf. Considerando (T) da Resolução.

Pretendendo uma maior transparência e confiança nestas novas tecnologias, considera-se (e bem) que deve ser introduzido um sistema de registo de robôs avançados no mercado interno da União, podendo este abranger todas (ou apenas determinadas) categorias de robôs[175], permitindo-se assim que qualquer sujeito que venha a interagir com um robô registado conheça da sua «natureza do fundo, dos limites da respectiva responsabilidade em caso de danos patrimoniais [...] e de todas as outras informações relevantes»[176]. Além disso, prevê igualmente a criação de um sistema de licenciamento de robôs inteligentes, que viria abranger tanto os seus criadores como os seus utilizadores[177].

De facto, uma implementação de um sistema de registo e um sistema de licenciamento de *softbots* poderia indubitavelmente permitir uma maior transparência e confiança na contratação, na medida em que a implementação de critérios estandardizados de teste de robôs em cenários da vida real poderia resultar numa melhor avaliação dos riscos implicados na sua utilização e, eventualmente, de um sistema de inspecção regular do *software* (e do *hardware*) dos mesmos, almejando assegurar o seu correcto funcionamento.

Ademais, é sugerida a hipótese de se averiguar a necessidade de uma revisão do Regulamento Geral sobre a Protecção de Dados (doravante 'RGPD')[178], na medida em que alguns aspectos ligados ao acesso a dados e à proteção de dados pessoais e da privacidade podem ainda estar por resolver e/ou persistirem preocupações quanto à garantia de privacidade no método de comunicação sem intervenção humana entre dispositivos e aplicações e/ou com bases de dados[179].

Salienta-se a necessidade de um conjunto de disposições legais que rejam, em particular, a responsabilidade, a transparência e a prestação de contas, tendo em vista que a nossa actual realidade já conta com grandes avanços tecnológicos, que viabilizaram a atribuição de certas capacidades aos robôs que, até então, eram

175 Cf. Considerando (2) da Resolução e §Registo de «robôs inteligentes» do Anexo da Resolução.
176 Cf. alínea e) do Considerando (59) da Resolução.
177 Cf. Considerandos (W), (9) e (23) da Resolução e §Licença para os Criadores e §Licença para os Utilizadores do Anexo da Resolução.
178 Cf. Regulamento (UE) 2016/679, de 27 de Abril, do Parlamento Europeu e do Conselho, 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 Directiva 95/46/CE.
179 Cf. Considerandos (N), (10), (13), (14) e (18) e seguintes da Resolução.

exclusivas ao Homem, devendo esta questão ser igualmente resolvida ao nível da União, «a fim de garantir o mesmo nível de eficácia, de transparência e de coerência na execução da segurança jurídica em toda a União para benefício dos cidadãos, dos consumidores e das empresas»[180].

Em virtude quer do facto de que será tanto mais difícil a equiparação do robô a um mero instrumento do seu utilizador quanto maior for a sua autonomia, quer do facto de lhes poder ser atribuída a capacidades de auto-aprendizagem e adaptabilidade, questiona-se se o actual regime ordinário em matéria de responsabilidade é suficiente para resolver os eventuais problemas, ou se será necessário um novo complexo de normas e princípios que venha clarificar a responsabilidade jurídica dos vários intervenientes quanto à responsabilidade por actos ou omissões dos robôs «quando a causa não puder ser atribuída a um interveniente humano específico e os actos ou as omissões dos robôs que causaram os danos pudessem ter sido evitados»[181].

Mais ainda, sublinha-se que as normas tradicionais não estão preparadas para resolver os problemas da responsabilidade jurídica pelos danos causados por um robô, por não ser possível identificar a parte responsável para prestar a indemnização e para lhe exigir que reparasse os danos causados. Evidencia-se também a intrínseca complexidade dos problemas de responsabilidade objectiva suscitados por danos causados por robôs capazes de auto-aprendizagem e de adaptação, na medida em que se acentua o grau de imprevisibilidade da actuação do robô. Perante isto, é sugerido que os robôs deveriam ser dotados de uma «caixa negra», onde seriam registadas todas as operações realizadas, desde a sua concepção até à sua efectiva realização[182].

Dada a falta de soluções legais adequadas para os problemas referidos na Resolução, é recomendada a adopção de um regime de seguros obrigatórios como uma potencial solução para acautelar os interesses daqueles que sofreram danos causados por robôs, e de um fundo de garantia de reparação de danos não abrangidos pelo seguro, devendo o regime do seguro ter em consideração todos os elementos potenciais da

180 Cf. Considerando (49) da Resolução.
181 Cf. Considerando (AB) da Resolução.
182 Cf. Considerandos (Q), (U), (Y), (Z), (AB), (AD) a (AI), (12) e (53) a (55) da Resolução.

cadeia de responsabilidade (sendo por isso mais abrangente que um regime de automóveis)[183].

Por fim, uma última nota relativamente à Resolução: não fossem já todas as sugestões apresentadas pelo Parlamento de se louvar, vai este Instituto mais longe ao sugerir, nos seus Considerandos (AC) e alínea f) do (59), que, em última instância, poderia ser ponderada a hipótese de se criar uma nova categoria jurídica, «com características e implicações próprias»: a 'personalidade electrónica'.

Não existem dúvidas que todas as recomendações que salientámos são indubitavelmente inovadoras e ajustadas à realidade que vivemos, mas nem por isso nos parece que, em sede do tema que temos desenvolvido, se possa ir tão longe quanto à criação de uma 'personalidade electrónica'[184]. Entendemos, pelo contrário, que até melhor compreensão das capacidades/limitações da inteligência artificial, será bastante a criação de uma nova categoria jurídica que atribua, como já se sugeriu[185], uma capacidade de agir limitada às capacidades de actuação do *software* que não assente na personalidade jurídica.

183 Cf. Considerando (57) e alíneas a) a c) do Considerando (59), ambos da Resolução.
184 No mesmo sentido, cf. M. BARBOSA, *op. cit.*, pp. 204-209.
185 V. supra §4.3 A qualificação jurídica dos agentes de *software*.

7.CONCLUSÃO

Aqui chegados, torna-se difícil negar que nos aproximamos de uma realidade tecnológica e, possivelmente, juridicamente, nova. Pelo contrário, evidencia-se uma crescente preocupação com a previsão de soluções novas para um futuro que se avizinha mais rápido do que se pensa.

É verdade que no desenvolvimento deste trabalho ocupámo-nos grandemente sobre o funcionamento da tecnologia e dos problemas que o recurso a esta convocaria no âmbito da contratação electrónica. Não obstante, cumpre-nos reiterar que as DLT não se limitam (nem têm que se limitar) apenas a sistemas de pagamento descentralizados e à contratação; diferentemente, estão em curso projectos-piloto de diversas áreas que recorrem ao uso desta tecnologia, nomeadamente em sistemas de gestão e distribuição de energias renováveis[186], na indústria hospitalar e farmacêutica[187], no âmbito do registo predial[188], em sistemas de votação *online*[189], entre muitos outros. Perante a versatilidade desta tecnologia, fez-se referência à mais recente Lei-Modelo da Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), no âmbito da contratação electrónica, a Lei-modelo sobre documentos transmissíveis electrónicos.

Neste contexto, concluímos que o recurso a esta tecnologia no âmbito da contratação electrónica constitui, de facto, uma nova forma de contratar, podendo ser adoptada a denominação 'criptocontratação', uma vez que, por um lado, não se identifica com a contratação automatizada com recurso à EDI (desde logo pela inexistência de um acordo-tipo prévio entre as partes contratantes), e, por outro, se trata

186 Cf. NASDAQ (2018). *Estonia Launches Green Energy Blockchain Project*. Obtido em 30 de Janeiro de 2018, disponível em http://www.nasdaq.com/article/estonia-launched-green-energy-blockchain-project-cm904091.
187 Cf. United News of India (2018). *Blockchain-based healthcare setup 'Healthureum' launched.* Obtido em 30 de Janeiro de 2018, disponível em http://www.uniindia.com/blockchain-based-healthcare-setup-healthureum-launched/india/news/1120879.html.
188 Cf. J. YOUNG (2017). *Sweden officialy started using blockchain to register land and properties.* Obtido em 30 de Janeiro de 2018, disponível em https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties, J. WONG (2017). *The Encryption Technology of Automatic Teller Machine Networks.* Obtido em 30 de Janeiro de 2018, disponível em https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/.
189 Cf. S. HIGGINS (2017). 'Moscow Government Open-Sources Blockchain Voting Tool.' *Coindesk.* Obtido em 30 de Janeiro de 2018, disponível em https://www.coindesk.com/blockchain-voting-code-made-open-source-moscows-government/.

de uma forma de contratação electrónica automatizada que convoca a participação de agentes de *software* e ao recurso à criptografia para concluir negócios jurídicos sem intervenção humana. No entanto, depreende-se que, caso seja adoptada uma denominação própria para esta forma de contratar distinta daquela que propomos, dever-se-á optar por uma denominação tecnologicamente neutra.

Ademais, ainda que seja possível e justificável um enquadramento jurídico em que se contemple o agente de *software* enquanto representante do seu sujeito utilizador, entendemos que deve ser criado um regime próprio para regular a criptocontratação, visto que a actuação do agente de *software* levanta diversas dúvidas quanto à natureza jurídica da sua 'vontade', que por sua vez irá conduzir a problemas na aplicação do regime do erro-vício e do erro-obstáculo, alegadamente aplicável por força do disposto nos números 2 e 3 do artigo 33.º da LCE.

É que, no fundo, a grande diferença entre a contratação 'tradicional' e a criptocontratação reside no facto de na primeira se estipularem cláusulas contratuais para auxiliar a resolução *ex post* de eventuais conflitos que possam advir daquele negócio; já na última, codificam-se 'cláusulas contratuais' para que *ex ante* se previnam (tentativamente) todos os possíveis conflitos, sendo isso impossível como se sabe, já que «a lei é insuficiente: não pode[ndo] prever todas as situações com que a vida nos surpreende de quando em vez»[190].

Além disso, pelas dificuldades que acabámos de referir, igualmente difícil se revela a tentativa de identificação da parte responsável para prestar a indemnização e para lhe exigir a reparação dos danos causados por um robô, e a aplicação do regime da responsabilidade objectiva quando os danos sejam causados por robôs capazes de auto-aprendizagem e de adaptação. Aliás, neste sentido recomenda-se na Resolução que as Leis de Asimov[191] devam ser encaradas como dirigidas aos humanos, apoiando-se precisamente na dificuldade em traduzir e incorporar estes 'princípios' no código fonte do *software.*

Mais ainda, atenta a regra de não discriminação em razão do sujeito (que dispõe que não se poderá «limitar o tipo ou a extensão dos danos a indemnizar nem as formas

190 Cf. A. Santos JUSTO (2003). Introdução ao Direito, pp. 122-123.
191 Cf. I. ASIMOV, *op. cit.*, loc. cit..

de compensação [...] pelo simples facto de terem sido provocados por um agente não humano»[192]), entendemos ser justa e adequada considerar a implementação de sistemas de registo, classificação, licenciamento e revisão periódica dos agentes de *software* e da adopção de um regime de seguros obrigatórios (como potencial solução para acautelar os interesses daqueles que sofreram danos causados por robôs), assim como de um fundo de garantia de reparação de danos não abrangidos pelo seguro, devendo o regime do seguro ter em consideração todos os elementos potenciais da cadeia de responsabilidade.

Por fim, entendemos ser razoável a criação de uma nova categoria jurídica, ajustada aos agentes de *software* e que lhe atribua uma capacidade de agir limitada às suas capacidades de actuação, diferente de uma 'personalidade electrónica'.

192 Cf. Considerando (52) da Resolução.

SMART CONTRACTS : POSSÍVEL SOLUÇÃO PARA A RELUTÂNCIA EM ENTRAR NUM CONTRATO EM AMBIENTE *ONLINE*?

JOSÉ BELO [1]

1 José Belo é licenciado em Direito pela Universidade de Coimbra. Possui as certificações CIPP/E e CIPM através da IAPP e, ainda, a certificação em Law & Technology da Faculdade de Direito da Universidade da Califórnia em Berkeley. Actualmente, é *Of Counsel* em matérias relacionadas com Direito da Privacidade e Protecção de Dados para Teófilo Araújo Santos - Advogados. É, presentemente, membro da IAPP (EUA), sendo *co-chair* para a KnowledgeNet de Lisboa, Portugal. josebelo@teofilosantos.pt

RESUMO

Olhando para o comércio *online*, quando comparado com o comércio offline, e apesar do seu constante aumento ao longo dos anos, o que se torna evidente é que continuamos, esmagadoramente, a comprar como sempre comprámos: em lojas, em supermercados, em centros comerciais. Por muito que a Internet, como mercado de bens e serviços, seja cada vez mais, utilizada, as estatísticas, no entanto, demonstram uma realidade diferente. No artigo, procura-se circunscrever o fundamento para esta assimetria entre o mercado tradicional e o mercado *online* à confiança, definindo-a como uma anomalia. De seguida, olhar-se-á, de forma crítica, para os *smart contracts* (contratos inteligentes), baseados em tecnologia *blockchain*, como possível solução para esta anomalia. Para além disso, analisar-se-á se as características dos contratos inteligentes, que são autoexecutáveis, poderão permitir uma mudança de paradigma da Lei, nomeadamente, na Lei dos Contratos.

Palavras-Chave: Contratos, *Blockchain*, *Smart Contracts*, *Self-driving contracts*, Comércio *online.*

1. INTRODUÇÃO [1]

Thomas S. Kuhn define a mudança de paradigma na ciência normal como a solução para uma crise científica que leva a uma "*reorientação científica*"[2]. Este artigo procura dar uma visão da tecnologia *blockchain* numa das suas adequações legais mais prementes - os contratos inteligentes, ou *smart contracts* - como sendo potenciadores de uma mudança de paradigma dentro da Lei dos Contratos, que deve ser olhada como uma solução para uma crise da ciência jurídica normal que está a emergir com o advento da Internet e, nomeadamente, da evolução tecnológica que a rede permite.

Esta tecnologia tem, então, sido actor invisível, mas fulcral, na revolução em que está inserido, enquanto tecnologia disruptiva que é, capaz de, *per se*, causar um movimento tectónico no edifício jurídico actual suficientemente concreto para lhe criar fendas. Bem como suficientemente qualificado para ser *the new normal*, fornecendo uma resposta, que ainda não está adequadamente solidificada, mas que tem o potencial de ser uma nova solução para uma anomalia, entendida na perspectiva de Kuhn, que permanece subvalorizada na entrada em contratos em ambiente *online*, visto a crise ser puramente digital e afectar, apenas, contratos puramente digitais. A anomalia permanece silente porquanto os contratos puramente digitais de âmbito mais generalizado não representam, de todo, uma parte muito significativa da criação contratual que as partes tendem a estabelecer.

Aliás, corroborando a precisa analogia da teoria científica de Kuhn com as alterações performativas que a tecnologia *blockchain*, no geral, e os *smart contracts*, em especial, aparentemente infligem nos princípios legais e na legalidade no seu todo, concordamos com Habermas, ao aplicar a supramencionada terminologia de Kuhn à Lei, estabelecendo uma concreta correspondência entre o paradigma da ciência normal e o paradigma da Lei. Assim, para Habermas, o paradigma da Lei consiste na "*visão exemplificativa de uma comunidade legal em relação a como o sistema de direitos e de*

1 Nota : Todas as traduções de inglês para portugês foram realizadas pelo autor do artigo, procurando ser o mais fiel possível ao original.
2 KUHN, Thomas S., "*Structure of Scientific Revolutions*", University of Chicago (1962)

princípios constitucionais pode ser actualizado no contexto perceptível de uma determinada sociedade[3]*".*

Habermas acrescenta, ainda, que "*um paradigma de lei advém de um modelo de sociedade contemporânea para explicar como direitos e princípios constitucionais devem ser concebidos e implementados se, no contexto actual, eles devem preencher as funções normativamente atribuídas a estes",* com a sociedade, no seu contexto actual, a ser ela a definir como esses direitos e princípios constitucionais devem ser compreendidos.

Assim, Habermas define um paradigma de lei como ciência normal para a sociedade a quem as normas são destinadas, e que são por esta aceites, através da contextualização das normas no enquadramento societário que estas pretendem regulamentar, assumindo e considerando a Lei como uma resposta historicamente específica às acepções e preocupações da sociedade naquele momento.

O propósito deste artigo é o de definir, em termos gerais, o que são contratos inteligentes (*smart contracts*), os princípios que os fundamentam e a legalidade que os sustenta, a anomalia que circunscrevemos na Lei de Contratos actual e os seus efeitos numa sociedade cada vez mais digital. Ainda, analisar-se-á se os contratos digitais potenciam uma mudança de paradigma na percepção actual da Lei que os contratos inteligentes, e uma apreciação sobre o papel que esses podem ter nos resultados contratuais tradicionais que tem regido a relação entre a sociedade e as normas.

Na verdade, é a última premissa do artigo que consubstancia a possibilidade de existência de uma mudança de paradigma, visto que os resultados contratuais tradicionais podem erodir com a possibilidade de haver contratos que se impõem por si

3 HABERMAS, Jurgen, "*Faktizitiat und Geltung: Between facts and norms - contributions to a discourse theory of Law and Democracy*", MIT Press, 1996, page 195. Ver ainda DE VRIES, Ubaldus, "*Kuhn and Legal Research - A Reflexive Paradigmatic View on Legal Research",* Recht en Methode in onderzoek en onderwijs, Vol. 3, n.º 1 (2013), nomeadamente, quando refere que "*quando os problemas acontecem ao nível da sociedade, a crença fundamental na capacidade da Lei para os resolver é abalado; estes desenvolvimentos não podem ser justificados mas tornam-se "anomalias de Kuhn". Estas anomalias podem ser explicadas através de uma atitude reflectiva direccionada às premissas da Lei e isto pode ser feito se o objecto de estudo não se limitar, apenas, à Lei mas no local e no momento em que estas anomalias aparecem, incluíndo o seu meio ambiente, de forma a fazer sentido quanto a problemas estruturais; para compreender de onde surgem estes factos, o que os fez surgir, o que os torna tão singulares? A teoria social é, assim, um meio complementar para fazer sentido destes novos problemas com que a Lei se depara.*"

só, sem ser necessário, no seu todo ou em parte, de intervenção de terceiros, *máxime* o Estado, para obrigar as partes ao seu cumprimento ou ao ressarcimento dos danos pelo seu não cumprimento.

No entanto, o artigo também analisará se tal erosão é conclusiva e restringida ou se a tecnologia irá, igualmente, causar uma mudança mais vasta de paradigma relativamente à execução para cumprimento compulsivo de um contrato, mediante um poder público e relativamente aos princípios gerais da Lei que fundamenta essa execução compulsiva ou respectiva sanção indemnizatória, a existir.

Desta forma, focar-nos-emos em aferir se existem premissas para uma nova revolução científica nas ciências legais, trazida pelo advento da Internet e da capacidade tecnológica que esta consubstancia, nomeadamente, pela implementação de contratos inteligentes. Questiona-se, no fundo, se os contratos inteligentes são o *fumus* de uma mudança na ciência normal, promovendo uma oscilação dos pilares fundamentais da Lei dos Contratos, que se mantiveram, até este ponto, no tempo e na arte.

De facto, até aqui, os contratos tradicionais têm sabido resolver as questões para os quais foram criados, maioritariamente contendo necessidades de estabelecimento de direitos e obrigações, no mundo não-*online*, entre as partes. No entanto, com a Internet e a globalização das partes, e das respectivas jurisdições onde estas residem, os contratos tradicionais poderão ser, questiona-se, insuficientes para responder ao ritmo que a tecnologia tem imposto à sociedade e ao que a fundamenta, para lá da questão central da confiança.

Com este artigo, pretende-se, a mais, compreender como a ciência normal dos contratos e os princípios que lhes servem de suporte não parecem suficientes para permitir a contratação em ambiente *online* com a frequência que seria desejada, limitando a expansão do mercado digital e o estabelecimento das consequentes relações contratuais. Com a tecnologia *blockchain* e os contratos inteligentes, no entanto, enfatiza-se esta alteração, ainda mais, com soluções tecnológicas que estão, hoje, ao dispor de qualquer jurista, criando as condições para que a mudança de paradigma, inevitavelmente, aconteça, no presente e, de forma mais reiterada, num futuro muito próximo.

Igualmente, propõe-se uma análise crítica em relação aos contratos inteligentes, enquanto solução tecnológica e prática que poderá causar o fim de uma anomalia, que os contratos actuais não parecem conseguir resolver: a falta de confiança entre as partes para entrar num contrato em ambiente digital.

Desta forma, olhar-se-á para o comércio digital como exemplo paradigmático disso mesmo. Desde as características que delimitam a crise na contratação no comércio digital, a evolução histórica que demonstra a existência da crise, culminando nas principais razões para a mesma. Tentar-se-á, igualmente, delimitar o paradigma legal actual enquanto fundamento para a falta de confiança para entrar num contrato (a anomalia, que persiste), olhando para os contratos inteligentes como uma possível solução para essa anomalia, causando, ao mesmo, tempo uma crise no paradigma legal actual. E, potencialmente, ao permitir resolver, em parte, a crise, promover uma revolução mais ampla no estado da Lei actual, em direcção a um evolutivo paradigma legal que permita absorver as possibilidades introduzidas na sociedade, e na forma como esta se relaciona, pela tecnologia nos últimos anos.

Logo, a tecnologia blockchain, quando olhada pelo prisma da crise em que se encontram os contratos *online* e pelo prisma da metodologia proposta por Kuhn e, paralelamente, por Habermas, cumpre a última fase dessa metodologia, permitindo ao indivíduo "*uma nova forma, agora finalmente estruturada, de dar ordem aos dados"*, servindo como resposta à anomalia que lhe deu origem, numa parte da transição para um novo paradigma, que, no entendimento de Habermas sobre a questão, uma mudança de paradigma normativo.

2. *SMART CONTRACTS* OU CONTRATOS INTELIGENTES: NOÇÃO GERAL

A primeira vez que o termo "*contrato inteligente"* foi utilizado aconteceu no artigo "*Formalizando e assegurando relações em redes públicas*", de Nick Szabo, em 1997. Considerando o contrato o "*alicerce básico de uma economia de mercado*",

Szabo propõe uma evolução ao contrato tradicional, que utilize as "*leis actuais, procedimentos e teorias"* mas que, ao mesmo tempo, "*reduz os custos mentais e transacionais associados, impostos quer pelas partes, quer por terceiros, quer pelas ferramentas que utilizam*", com o objectivo de definir uma "*nova forma de formalizar e assegurar relações digitais que são mais funcionais que os seus inanimados antecessores em papel*[4]".

Szabo dá, no artigo, um exemplo claro de como um contrato digital responde às exigências de formalização e de segurança no cumprimento do contrato, bem como à redução de custos, que lhe terá de ser característica. Definindo os contratos inteligentes como auto-executáveis, Szabo concretiza a sua visão com um contrato inteligente entre um comprador e um vendedor de um automóvel. Com um contrato digital de compra e venda do automóvel a crédito como exemplo, pode constar no contrato inteligente um protocolo que assegure a protecção do credor em caso de falta de pagamento.

Assim, quando o comprador "*falha um pagamento, o contrato inteligente invoca o protocolo da posse do automóvel por falta de pagamento, devolvendo o controlo das chaves do automóvel ao* [credor]*",* quando tal for seguro de realizar. "*Este tipo de protocolos pode ser muito mais barato e muito mais eficaz"* que qualquer outro mecanismo actual à disposição de um credor, evitando um processo judicial, os custos associados, bem como o tempo que demorará entre a falta de pagamento e a restituição do automóvel, caso persista a falta de pagamento da ou das prestações devidas.

A solução de Szabo não viola a vontade das partes porque todos estão informados das consequências dos seus actos: o contrato tem cláusulas que não mudam e que são pré-negociadas entre as partes[5]. Ao comprador é dado, então, conhecimento que a falta

4 SZABO, Nick, "*Formalizing and Securing Relationships on Public Networks",* First Monday Peer-reviewed Journal of the Internet, Vol. 2, Number 9 (September 1997)

5 Existe outro tipo de contratos inteligentes, com características diferentes dos contratos inteligentes aqui analisados, denominados de *self-driving contracts.* Estes contratos caracterizam-se por i) as partes definirem apenas objectivos *ex ante* amplos; mas ii) o contracto usa ferramentas de análise computacional e inteligência artificial para traduzir os objectivos gerais *ex ante* em termos específicos, denominados de directivas, que entram em vigor na altura do cumprimento do contrato e que são ajustados, consoante a análise computacional e as decisões da inteligência artificial, enquanto o contrato está em vigor, de forma a melhor se atingir o objectivo; onde iii) aqueles termos são baseados em dados obtidos após as partes darem início ao cumprimento do contrato. Assim, de uma forma muito primária, são dois os termos iniciais destes contratos auto-dirigidos que têm de ser acordados pelas partes, i) o objectivo pretendido; e ii) como dividir os dividendos. À medida que o contrato é executado, é a inteligência artificial que decide todos os outros elementos do contrato, de forma a melhor atingir o objectivo pretendido. Para isso, a inteligência artificial capta dados e informação sobre o estado actual do Mundo, à altura da execução do contrato, e faz

de pagamento dentro do prazo determina a sua imediata perda de controlo de acesso do carro, o que, no fundo, servirá como um incentivo muito forte para o cumprimento. E para o credor, tal conhecimento é uma forma muito clara de saber-se consciente de que, caso haja alguma falta de pagamento, o procedimento é imediato e automático, evitando todos os custos associados, em termos de horas de trabalho, expediente, ou outros, directa ou indirectamente, conexos com processos judiciais ou quaisquer outras formas previstas de reaver ou o bem ou o pagamento em falta.

Os contratos digitais propostos por Szabo não colidem com os princípios estabelecidos nas origens do Cristianismo, onde os Cristãos se comprometiam a cumprir com as suas promessas. Igualmente, não colidem com a Lei Romana, onde as promessas privadas têm de ser realizadas ("*pacta sunt servanda*")[6]. No entanto, a construção contratual de Szabo coloca em causa princípios basilares do direito dos Contratos, como a necessidade de intervenção judicial.

Thomas Hobbes refere, na sua obra "Leviatã", que "q*uando se faz um pacto em que ninguém cumpre imediatamente sua parte, e uns confiam nos outros, na condição de simples natureza (que é uma condição de guerra de todos os homens contra todos os homens), a menor suspeita razoável torna nulo esse pacto. Mas se houver um poder comum situado acima dos contratantes, com direito e força suficiente para impor seu cumprimento, ele não é nulo[7]".*

Grócio, igualmente, partindo da "*pacta sunt servanda*" romana, desenvolve o princípio da inviolabilidade dos contratos, exigindo ao Estado não só uma dimensão

previsões sobre que acções as partes devem tomar para melhor atingir o objectivo por estas estabelecido, e, depois, dirigir as partes para cumprirem com essas acções. Também identifica os dividendos e direcciona as partes para o dividirem de acordo com a forma que estabeleceram *a priori.* Assim, não só a inteligência artificial monitoriza o estado do Mundo (economia, sociedade, cultura, preço das acções, tempo, calendário, o que for necessário) como também monitoriza o comportamento das partes. À medida que o Mundo muda, a inteligência artificial altera as directivas, nunca perdendo de vista os objectivos ou como melhor chegar a eles, permitindo uma flexibilidade contratual impossível nos rígidos contratos tradicionais mais comuns, onde a definição de todos os direitos e obrigações são estabelecidos antes da assinatura do contrato, tendo em conta qualquer alteração das circunstâncias de facto como forma de não prosseguir o contrato ou como cláusula de exclusão de responsabilidade em caso de incumprimento sem culpa ou negligência. Para mais sobre contratos auto-dirigidos, ver CASEY, Anthony J. e NIBLETT, Anthony, "*Self-Driving Contracts",* Working Paper, 1 de Março de 2017 (última revisão em 4 de Fevereiro de 2018), disponível em SSRN : https://ssrn.com/abstract=2927459 ou http://dx.doi.org/10.2139/ssrn.2927459

6 Ver SHARP, Malcolm P., "*Pacta sunt servanda",* Columbia Law Review, Vol. 41, n.º 5 (May 1941), pp. 783-798

7 HOBBES, Thomas, "Leviatã", Capítulo XIV, Imprensa Nacional Casa da Moeda, Portugal, 2010, parágrafo 18

negativa de não intromissão no que as partes acordam entre si, mas, principalmente, uma dimensão positiva, onde é exigido ao Estado garantir os direitos e deveres estabelecidos contratualmente pelas partes[8].

Pense-se, por exemplo - de forma muito simplificada e sem ter em consideração as protecções legais existentes para casos semelhantes - o caso de um locatário que não paga as suas rendas. Com um contrato inteligente, não só se torna desnecessário todo o processo que leve ao despejo do locatário, como o contrato cessa por força do próprio contrato, que obriga as partes, e que as partes assinaram de livre vontade.

Deixa, por isso, de ser necessário, ao locador, recorrer à acção directa, que, como se sabe, não faz cessar o contrato de locação, visto que, havendo um direito pessoal de gozo que onera a propriedade, a restituição desse direito de gozo ao locador só acontece com a sentença condenatória do locatário, provado o incumprimento deste.

Como deixa de valer ao locatário o esbulho, por o contrato prever, quantas vezes for necessária, a restituição da posse ao locador de várias maneiras possíveis: alterando o código de acesso à fechadura da moradia, devolvendo todos os contratos de água, luz, gás, televisão ou internet do imóvel ao locador ou controlando, em imóveis preparados como *smarthomes,* o acesso a janelas, persianas, electrodomésticos, inviabilizando qualquer vontade do locatário incumpridor de prosseguir com qualquer acção violenta para retomar a posse do imóvel sem acrescentar uma pesada herança financeira, seja destruído o que está, seja adquirindo alternativas, ao incumprimento já existente pelo não pagamento das rendas.

Para além disso, evita-se que a acção de despejo leve a que o locador deixe de receber qualquer renda que lhe seja devida após a entrada da acção em Tribunal, pela ausência de património do locatário para satisfazer as rendas já vencidas, bem como os juros vencidos e vincendos.

8 Ver GROTIUS, Hugo, "*The Law of War and Peace"*, Universal Classics Library - Autograph Edition, M. Walter Dunne, 1901. Ainda, WEBER, Max, "*Economia e Sociedade - Fundamentos da sociologia comprensiva*", Vol. 2, Fundação Universidade de Brasília, 1999. Weber, na senda das posições de Hobbes e Grotius, refere que "*a organização estatal atual concede ao indivíduo (que, em princípio, é apenas seu objeto) meios para proteger seus interesses",* estabelecendo, no fundo, o *ius imperium* como solução última e omnipresente para conflitos em caso de incumprimento ou cumprimento defeituoso de contratos, a que as partes podem recorrer para fazer valer o que entendem ser os seus direitos, afectados e/ou restringidos por acções ou omissões da contra-parte no contrato.

Assim, com a necessidade actual de uma decisão judicial para fazer cumprir um contrato ou para o resolver, em comprovado caso de incumprimento, a solução de Szabo retira, em teoria, da equação a necessidade de um decisor externo, permitindo às partes a resolução da questão entre si. Ao mesmo tempo, através de um contrato inteligente, que as partes conhecem e que cumpre com a sua vontade, a resolução de um conflito que surja relativamente ao contrato é efectuada em tempo real, por cláusulas previstas e acordadas pelas partes que actuam independentemente de qualquer acção sua, o que previne o incumprimento do contrato por parte destas, cientes que estão dessas consequências automáticas.

3. *E-COMMERCE*, CONTRATOS E A QUESTÃO DA CONFIANÇA

3.1. Retalho *online* e tradicional : uma comparação

A promessa da Internet como um novo mercado global, onde a compra e venda de bens e serviços se torna (quase) imediata em todo o planeta é, em si, uma revolução absoluta na forma de o ser humano comprar e vender desde a sua génese e evolução, enquanto espécie.

Dependente que estava das suas deslocações físicas às redes de mercados, feiras ou de lojas há milhares de anos, hoje, o ser humano consegue comprar tudo o que quiser, sem ter de sair de casa, através da Internet. Desta forma, criou-se aquilo a que se designa como o mercado de *e-commerce*.

Uma comparação entre o mercado de retalho *e-commerce* e o mercado de retalho tradicional deve ter em consideração quatro dimensões de eficiência de mercados: nível de preços, elasticidade de preços, os custos de menu e a dispersão de preços[9].

A dimensão do nível de preços preconiza se os preços na Internet são mais baixos que nas lojas tradicionais. A dimensão da elasticidade de preços procura saber se os consumidores são mais sensíveis a pequenas alterações de preços na Internet. A dimensão dos custos de menu indaga sobre se os vendedores ajustam o preço dos

9 SMITH, Michael D., BAILEY, Joseph e BRYNJOLFSSON, Erik, "*Understanding Digital Markets: Review and Assessment",* MIT Press, Estados Unidos da América, 1999

produtos de forma mais pormenorizada ou mais frequentemente na Internet, quando comparado com o mercado tradicional. E, por último, a dimensão da dispersão de preços interpela se a diferença entre o preço mais baixo e o preço mais alto é maior ou menor na Internet, em comparação com o mercado tradicional.

Empiricamente, entende-se que a Internet deveria permitir um mercado mais eficiente, tendo em consideração a possibilidade de uma loja *online*, em abstracto, poder ter custos mais baixos que uma loja física - nomeadamente, não pagando rendas e funcionários em cada cidade; o acesso a um número de consumidores que é potencialmente tão grande quanto o número de pessoas que acedem à Internet; e a possibilidade de, caso se opte por vender produtos digitais, estes não estarem sujeitos a qualquer limite ou custos adicionais do lado da oferta, para lá dos custos de fabrico[10].

10 Com a *ficheirização* de produtos, como *software* (programas, apps, jogos, etc.), livros ou música, estamos perante uma alteração substancial das regras do jogo, no que toca a produtos. Se dantes, a compra de um produto estava dependente da disponibilidade do mesmo, que era limitada ao *stock* existente, hoje, os produtos digitais não têm qualquer limite de stock nem quaisquer limitações no que toca a armazenamento de stock, visto que a partir de uma única cópia se consegue replicá-la as vezes que forem necessárias para satisfazer a procura. Com estas incógnitas na equação, a promessa do comércio na Internet passaria por vender muito um produto a um preço baixo, de forma a permitir ao consumidor alterar a sua posição no mercado de um mercado onde produtos competem uns com os outros devido às limitações de rendimento de cada consumidor para um mercado não-competitivo onde os preços são tão baixos que é possível comprar mais do que um produto da mesma gama e onde as limitações de rendimento de cada consumidor são negligenciáveis. Para mais sobre esta posição, ver ANDERSON, Chris, "*A Cauda Longa - Porque é que o futuro dos negócios é vender menos de mais produtos",* Actual Editora, Portugal, 2007. A confirmar a teoria de Chris Anderson é o facto de que, segundo a Ecommerce Foundation, a esmagadora maioria dos produtos e serviços contratados *online* são para produtos com preços inferior a 100€. E, segundo a mesma Fundação, os consumidores afirma que o preço é fundamental na altura de decidir o que comprar, com 57% dos consumidores a dizerem que compram o produto com o preço mais barato que encontrarem. No entanto, mais de dez anos após a publicação da obra de Chris Anderson, é um dado adquirido que as plataformas de distribuição dos produtos digitais passou a ter um impacto enorme sobre a venda de tais produtos, quando o que se previra era que a Internet retirasse o "*middle man".* Hoje, é inequívoco que o iTunes, o Google Play, a Kindle Store ou a Steam, entre muitas outras plataformas de distribuição, são essenciais para as vendas de produto digitais. E que, com as plataformas de distribuição a não removerem os dois intermediários entre o criador e o consumidor (e.g. editoras e distribuidores), bem como todos os restantes custos associados (nomeadamente, marketing), os preços não deixam de ter incluídos neles a mesma estrutura que os preços das suas contrapartes físicas. A ideia primária de que a Internet iria abolir esta estrutura de preços, abolindo os intermediários, sabemos hoje, não é real nem possível. E que, mesmo com preços mais baixos, os rendimentos dos consumidores também caíram, não permitindo passar de uma cultura "*or"* para uma cultura "*and",* conforme previsto por Anderson. Acrescente-se a este quadro a pirataria *online* de produtos digitais, e a promessa de um mercado *online* robusto de produtos digitais ou ainda não se concretizou ou dificilmente se irá concretizar, mantendo-se as características actuais do mercado imutáveis, o que, tendo em conta que estamos a falar de tecnologia, não permanecerá imutável durante muito tempo. Para além disso, a questão dos *stocks* não é assim tão importante para os consumidores. No "*Global Online Consumer Report*" de 2017, a consultora KPMG determinou que só 14% dos consumidores se preocupam com a existência de stock do produto na tomada de decisão de o comprar (embora 33% considere que é importante saber se está em stock ou não, para saber se compram o produto ou não).

No entanto, estudos efectuados no início do século XXI, comparando retalhistas *online* e tradicionais, mostraram que a diferença de preços entre ambos é, praticamente, inexistente[11].

A razão para isto não é atribuída à ineficiência do mercado *online* mas ao facto de ambos, na prática, estarem adstritos a preços de revenda dos fabricantes ou dos seus distribuidores praticamente idênticos. A possível diferença entre preços *online* e aqueles que encontramos em lojas tradicionais seria, assim, definida pelos custos operacionais e pelas estratégias de preço, que os estudos consideraram serem uniformes em ambas as plataformas mercantis.

À medida que as décadas vão passando, a promessa da capacidade do mercado *online* alguma vez ultrapassar o mercado tradicional permanece tão só isso - uma promessa. Com um número total de 2.520 milhões de pessoas a usar a Internet no mundo inteiro em 2015 (ou seja, 45% da população mundial acima de 15 anos), só 1.436 milhões compram *online* (26% da população mundial acima de 15 anos com acesso à Internet).

A quota do mercado *online*, quando considerado como uma de duas partes do mercado total (que inclui *online* e tradicional), em 2015, é de apenas 7.0%. O que significa que, mesmo com a maturidade da Internet como mercado global a ser uma realidade, 93% das compras de produtos efectuada por toda a população mundial continua a ser feita no mercado tradicional[12].

As estatísticas de *e-commerce* da E-Commerce Foundation parecem seguir esta apreciação. Na União Europeia, onde 77% da população (631.3 milhões) tem acesso à Internet, as vendas *online* deveriam ser, empiricamente, superiores. No entanto, o que

---

11 Ver HO, Lee Guen, HAE, Young Kim e RAN, Hui Lee, "*Is the Internet Making Retail Transactions More Efficient? - Comparison of Online and Offline CD Retail Markets",* Yonsei University College of Business and Economics, Coreia do Sul; BAKOS, J. Yannis, "*Reducing Buyer Search Costs : Implications of Electronic Marketplaces",* Management Science Magazine, Vol. 43, N.º 12, Institute for Operations Research and the Management Sciences, Estados Unidos da América, 1997; COURTNEY, Richard H., e, por último, GENTRY, Douglas W., "*Pricing, Market Efficiency and Consumer Choice in the Internet Commerce",* Journal of Private Enterprise, Vol. 17, N.º 2, Association of Private Enterprise Education, Estados Unidos da América, 2002.

12 Ecommerce Foundation, "*European Ecommerce Report 2017"* (2017), acessível em https://www.eurocommerce.eu/media/142202/c_european_ecommerce_report_2017_v170623-published_28basic_29.pdf

se nota é que não só a procura de bens *online* não é tão grande como seria esperado, como do lado da oferta, esta se mantém bastante limitada.

Na verdade, do lado da oferta, e apesar do número de empresas a vender *online* continuar a subir ano após ano, os números indicam uma realidade diferente. Assim, só 18% das empresas da União Europeia vendem os seus produtos *online*, apesar de 77% das empresas de vendas a retalho terem presença *online*[13]. Paralelamente, do lado da procura, o crescimento do *e-commerce* tem decrescido desde 2010, com algumas excepções. Assim, se em 2010 o *e-commerce* cresceu 21.25%, em 2016, o *e-commerce* cresceu apenas 13.62%.

Para além disso, as lojas tradicionais continuam a ser o local preferido dos cidadãos europeus para fazer as suas compras. Desta forma, apenas 35% dos cidadãos europeus considera que, no futuro, as lojas tradicionais não serão um factor a ter em conta no momento de decidir onde comprar um produto - o nível mais baixo quando comparado com outros continentes e regiões[14]. *A contrario,* tal significa que um inesperado número de 65% de europeus permanecem certos que as lojas tradicionais continuarão a ter o papel vital nas relações *B2C*, que têm hoje[15].

Com o *Brexit*, estes números podem tornar-se ainda mais problemáticos para a Europa. O Reino Unido, sozinho, é o país onde mais se vende *online*, sendo responsável por 197 mil milhões de euros em vendas *online*, com a Alemanha a um distante segundo lugar, com apenas 86 mil milhões de euros em vendas *online*. O que significa que o mercado *online* alemão tem apenas a dimensão de 43% do mercado *online* do Reino Unido. A França, o terceiro maior mercado *online* da União Europeia, regista 82 mil milhões de euros em vendas *online*. Conjugando os dados, chega-se à preocupante conclusão que o mercado *online* do Reino Unido é, sozinho, superior, em termos de

13 Ecommerce Foundation, "*European Ecommerce Report 2017"* (2017)
14 Ecommerce Foundation, "*European Ecommerce Report 2017"* (2017). O valor de 35% de europeus que não concorda com a frase "*Eu vejo um futuro onde as lojas tradicionais não são um factor determinante em como compro os meus produtos*" é, significativamente, mais baixo que a média mundial, onde 43% concordam com a frase, mas, curiosamente, é muito próxima do mercado norte-americano, onde 37% dos norte-americanos não concordam com a frase. São, assim, os mercados da América Latina (55%), Médio Oriente, Turquia e África (54%) e Ásia Pacífico (48%) que consideram que a Internet permitirá, um dia, uma reviravolta na forma como compramos produtos. Não deixa de ser curioso, e de salientar, que os países com mercados *online* e taxas de penetração da Internet tradicionalmente considerados mais amadurecidos e informados, são aqueles que menos consideram que o retalho *online* dificilmente fará desaparecer o retalho tradicional.
15 Ecommerce Foundation, "*European Ecommerce Report 2017"* (2017)

volume de negócios, que a combinação dos segundo e terceiro mercados *online* da União Europeia.

Com o *Brexi*t no horizonte, as estatísticas de vendas *online* da União Europeia irão sofrer, assim, um enorme decréscimo. E, incomodamente para uma União Europeia que está a tentar disputar terreno no mercado digital com outras potências - nacionais, regionais e continentais - não se esperam grandes alterações, quer na Alemanha, quer na França, quer nos mercados de compras *online* de qualquer outro país da União, de forma a preencher o espaço deixado vazio pelo Reino Unido.

No caso particular de Portugal, com uma população com acesso à Internet estimada em 7.316.148 portugueses em 2016, 43% compra produtos *online*. No entanto, a taxa de crescimento do *e-commerce* nacional está a perder fulgor, mesmo que as vendas estejam a aumentar[16]. O cenário do mercado português acaba por ser uma *carbon copy* dos números citados para a União Europeia, sendo um bom exemplo de como o mercado *online*, mesmo após décadas em que os números de utilizadores da Internet e as taxas de penetração da Internet têm constantemente aumentado, em todos os Estados-Membros, deparamo-nos com o facto incontestável de que o mercado *online* não tem sabido capitalizar o aumento do número de potenciais consumidores. E, com isso, não tem conseguido aproximar-se, quanto mais substituir, o mercado tradicional.

3.2. A crise actual da contratação *online* no *e-commerce* e a confiança

A Internet actual tem alterado significativamente de uma Internet de Informação para uma Internet de Valor. A Internet deixou de ser caracterizada, apenas, por aquilo a que chamamos de *World Wide Web* - que contém milhões de Bibliotecas de Alexandria no seu vasto universo em rede; pela *cloud;* pelas redes sociais; ou pelo *e-mail*. Por mais poderosos que tais instrumentos sejam, e por mais legitimidade que tenham transmitido à Internet, hoje, a rede também se estabeleceu como pilar de um mercado de natureza global de bens e serviços disponibilizados fisicamente ou em formato digital. Ainda, estamos perante "*um mundo onde os objectos físicos se integram homogeneamente na rede de informação, e onde os objectos físicos podem tornar-se participantes activos*

16 Ecommerce Foundation, "*European Ecommerce Report 2017"* (2017)

de processos de negócio. [Um mundo onde] *serviços estão disponíveis para interagir com estes "objectos inteligentes" através da Internet, obter o seu estado e qualquer informação associada a estes, tendo em conta os requisitos de segurança da informação e de privacidade*[17]*".*

No entanto, como vimos, permanece presente uma anomalia, aparentemente pouco evidente, relacionada com a decisão de comprar *online,* em detrimento das compras em lojas tradicionais. Referimos que a mesma é pouco evidente, considerando aspectos empíricos como o constante crescimento de vendas *online* e a chegada a rendimentos próprios da geração imediatamente anterior aos *millenials*, que já passou parte da infância e a totalidade da sua adolescência com a Internet como parte integrante da sua vida.

São, desta forma, vários os factores que contribuem para a anomalia dos mercados *online* e de *e-commerce.* Sem os elencar a todos de forma exaustiva, centrar-nos-emos nos principais. O primeiro factor é o hiato de tempo a que os consumidores estão, actualmente, sujeitos entre o momento em que compram o produto e o momento em que o recebem. O segundo factor prende-se com o facto de haver custos extra e/ou surpresa no comércio *online,* de que é exemplo os custos de envio por via postal, as taxas aduaneiras ou custos de intermediário adicionados, apenas, no momento em que se confirma a compra (e, até aí, nunca explicitados ou quantificados). O último factor reside no facto de as compras *online* serem feitas, maioritariamente (e em muitos casos, exclusivamente), através de cartão de crédito.

Em conjunto, estes factores fazem com que as compras *online* tenham sido preteridas, por parte dos consumidores, a favor das compras nos mercados tradicionais, onde não há hiato de tempo entre a compra e a utilização do produto, não há custos extra ou surpresa, para lá do preço estabelecido e haver uma multiplicidade de formas de pagamento (dinheiro, cartões de débito, cartões de crédito, pagamento a prestações, pagamento com cheque, entre outros).

17 HALLER, Stephen, KARNOUSKOS, Stamatis e SCHROTH, Christoph, "*The Internet of Things in an Entreprise Context",* em "*Future Internet Symposium",* Springer Berlin Heidelberg, Alemanha, 2008, pag. 15

Todos estes factores podem ser explicados e colocados dentro das quatro dimensões referidas *supra*, tendo em conta a taxonomia de dimensões definidas por Smith, Bailey e Brynjolfsson. No entanto, há uma dimensão que Smith, Bailey e Brynjolfsson não abordam, e que, na nossa opinião, é a primordial causa para a diferença enorme que permanece entre comércio *online* e comércio tradicional: a confiança.

Por maior que seja a promessa de um mercado global *online*, que permitiu em 2000 a bolha especulativa das *dot-com*[18], a verdade é que o mercado *online* não tem tido capacidade, sequer, de se tornar uma alternativa credível, incapaz de alterar a tendência de escolha do consumidor pelo mercado tradicional como mercado preferido, enquanto veículo de troca de rendimentos por bens e serviços. A bolha *dot-com* rebenta entre 2001 e 2002, num duro acordar para a realidade, onde os preços de acções ligadas à tecnologia caíram abruptamente. Várias explicações são dadas para o início do rebentar da bolha. A mais verosímil será a que é comum ao final de (quase) todas as bolhas: existe uma racionalidade individual dos investidores detentores de acções no momento

18 Em 1999, a criação das primeiras lojas *online* fez com que houvesse um consenso generalizado que estas iriam substituir as lojas tradicionais, tornando-se o pensamento dominante dos investidores desta altura. Tal pensamento dominante levou a um frenético investimento que produziu a, hoje conhecida como, bolha especulativa das *dot-com*. Quando implodiu, entre 2001 e 2002, produziu um dos mais audíveis rebentares de uma bolha especulativa de que há memória. O conceito das lojas *online* parecia simples: vender produtos do dia-a-dia a qualquer pessoa em qualquer momento, com tudo automatizado do lado do vendedor. A Pets.com era uma destas lojas. Com milhões de donos de animais de estimação só nos Estados Unidos da América e com o número de utilizadores da Internet a aumentar exponencialmente, o número de potenciais consumidores que utilizariam a Pets.com não parava de crescer dia após dia. Com uma forte campanha de marketing e investidores como Jeff Bezos, da Amazon, com quem a Pets.com estabeleceu uma parceria, todos os elementos principais de uma história, que só poderia acabar em sucesso, estavam alinhados. A pets.com tinha investidores de renome, uma boa campanha de marketing, uma base de potenciais clientes enorme e vendiam produtos muito populares. No entanto, de acordo com Matulich e Squires, no seu estudo sobre o que aconteceu com a Pets.com, os princípios básicos que estavam por detrás do modelo de negócio da Pets.com eram tudo menos estáveis. Com uma política forte de descontos e de baixos custos de envio para o consumidor, para atrair clientes, bem como uma fortíssima (e cara) campanha de publicidade, necessária para a activação da marca, a Pets.com registou, de Fevereiro de 1999 até Setembro desse ano, perdas operacionais de 20 milhões de dólares, com receitas de apenas 619.000 dólares. Ken Casser, analista da Jupiter Communications, explicou que "*o problema fundamental da Pets.com é que o seu modelo de negócio, nomeadamente na gestão dos custos, só funcionaria se tivesse um enorme volume de vendas".* Embora estes problemas fundamentais fossem evidentes a quem quer que olhasse para as contas da empresa, a sua entrada triunfal como empresa cotada na Bolsa de Nova Iorque, em Fevereiro de 2000, permitiu à empresa resolver os seus problemas de capital e para aumentar os custos de promoção da marca. Como Kirk Cheyfitz disse de forma eloquente, na sua obra "*Thinking Outside the Box - The 12 Timeless Rules for Managing a Successful Business", "o encantador fantoche ensinou ao mundo uma lição de negócios crítica: quando constróis uma marca que não faz dinheiro, o que se obtém em troca é nada".* Ver MATULICH, Erika e SQUIRES, Karen, "*What a Dog Fight: TKO: Pets.com*", Journal of Business Case Studies (JBCS), Vol. 4, n.º 5, Estados Unidos da América, 2008, disponível em https://www.cluteinstitute.com/ojs/index.php/JBCS/article/view/4779; e CHEYFITZ, Kirk, "*Thinking Outside the Box - The 12 Timeless Rules for Managing a Successful Business",* Simon & Schuster, Estados Unidos da América, 2003

em que apreciam o estado do mercado accionista[19]. No caso da bolha da Internet, a decisão racional dos investidores fundamenta-se no facto de estes se aperceberem que o preço das acções está suficientemente alto para lhes permitir um retorno significativo, relativamente ao investimento original realizado. No entanto, os valores das acções mantiveram-se elevados após as vendas dos investidores iniciais, significando isso que, por cada investidor satisfeito com o retorno do seu investimento, existia outro, com um sentimento optimista, mas, em retrospectiva, equívoco, de que o valor das acções ainda não tinha atingido o seu máximo.

Provavelmente motivados pelo "*FOMO*" ("*Fear Of Missing Out*"), fenómeno que temos visto, recentemente associada à *bitcoin*, esta segunda vaga de investidores não está a olhar para os fundamentais da empresa (fluxos de caixa, custos, clientes, vendas, receitas e despesas) mas para a expectativa de que a promessa do mercado *online* fará com que tais empresas obtenham lucros num futuro relativamente distante. Isto apesar de, no presente, a maioria das empresas tecnológicas apresentarem custos elevados sem receitas que os equilibrem, resultando em prejuízos avultados e poucos clientes, apesar de excessivos orçamentos para *marketing*. Como hoje sabemos, os lucros não aconteceram e a bolha das *dot-com* acaba por ter o fim de todas as outras bolhas, com as decisões de venda a não encontrarem resposta em decisões de compra para o valor pretendido, provocando a inevitável queda dos preços das acções.

Uma das vítimas colaterais mais importantes do rebentar da bolha das *dot-com* entre 2001 e 2002 é a confiança do público em relação ao mercado *online*. Um abalar de confiança do qual, como nos parece evidente, a população, em geral, ainda não recuperou.

Erkii Liikanen, Comissário Europeu para a Indústria, Empreendimento e PMEs de 1999 a 2004, referiu, num discurso para uma plateia de *insiders*, que quando "*não há confiança, não há transacção*[20]*",* demonstrativo de que a Comissão Europeia estava

19 ASPAROUHOVA, Elena, BOSSAERTS, Peter e TRAN, Anh, "*Market bubbles and crashes as an expression of tension between social and individual rationality: experiments*", Working Paper, 18 de Maio de 2011, página 2, disponível em https://pdfs.semanticscholar.org/531e/4138238a40cccd443484c79acd9462f60dcf.pdf. No mesmo sentido, FLOOD, Robert e GARBER, Peter M., "*Speculative Bubbles, Speculative Attacks and Policy Switching*", Massachussets Institute for Technology Press, Boston, Estados Unidos da América, 1994.

20 LIIKANEN, Erkii, "*Trust and security in electronic communications : The European contribution",* discurso proferido na "Information Security Solutions Europe Conference", Barcelona, 29 de Setembro de 2000, disponível em http://europa.eu/rapid/press-release_SPEECH-00-344_en.htm

ciente de que a anomalia existia e que tentaria, através de regulamentação, aumentar, de alguma forma, a confiança no comércio *online*. No entanto, a solução da Comissão Europeia para a questão foi tudo menos feliz. A Directiva 1999/93/CE, que estabelecia objectivos claros aos Estados-Membros para que estes fomentassem a utilização de assinaturas e certificados digitais reconhecidos legalmente, não surtiu o efeito desejado, nomeadamente, não estabelecendo as ferramentas capazes de gerar a confiança necessária nos europeus, para que estes entrem em transacções comerciais *online*.

Swinyard e Smith chegaram a conclusão semelhante, embora usando terminologia diferente: a razão substancial para os consumidores não comprarem *online* é o medo, fundamentando que "mais de *70% dos não-consumidores online - e mesmo um terço dos consumidores online - concordam com a afirmação "Eu não quero dar o meu número de cartão de crédito a um computador". Três quartos dos não-consumidores - e perto de metade dos consumidores online - concordam com a afirmação "Preocupo-me com o facto de o meu número de cartão de crédito possa ser roubado na Internet". Se estes medos puderem ser minimizados, um substancial aumento nas despesas globais no mercado de e-retalho poderá ser alcançado*[21]*".* Apesar de usarem a expressão "medo", parece-nos, no entanto, mais ajustada a expressão "falta de confiança" para descrever os factores assinalados por Swinyard e Smith.

Com mais de 10 anos passados desde a compreensão da anomalia da confiança no *e-commerce*, é empiricamente perceptível que pouco se alterou nas práticas comerciais e no respectivo enquadramento regulamentar, que permitisse medidas e soluções de segurança ou alternativas de pagamento credíveis e geradoras de confiança nos consumidores, relativamente às que existiam nessa altura. Apesar do comércio permanece obstinado a permanecer firme em relação ao cartão de crédito como instrumento financeiro para a entrada num contrato de compra e venda no mercado *online*, Newman e Bach, com os quais concordamos, consideram que, do lado legislativo, quer os E.U.A., quer a União Europeia têm a sua quota-parte de responsabilidade. Isto porque, apesar de terem abordagens diametralmente diferentes em relação ao *e-commerce* - autorregulação legalista nos E.U.A. e coordenação do

21 SWINYARD, William R. and SMITH, Scott M., "*Why people (don't) shop online: a lifestyle study of the Internet consumer",* Psychology & Marketing, 20, 7, July 2003, pp. 567–597.

comércio através de regulação normativa na União Europeia - quer um, quer outro coloca *"demasiada fé na capacidade do e-commerce de se autorregular*[22]*".*

Deve ser assinalado que existiram várias tentativas em restabelecer a confiança nos pagamentos através da Internet, especialmente com intermediários, como a Paypal. No entanto, os intermediários surgem, maioritariamente, como uma extensão das formas de pagamento já existente e que tanta falta de confiança provocam ao consumidor na Internet: a utilização dos cartões de crédito como forma de entrada no sistema.

Desta forma, é incontestável que uma anomalia existe e que impede a entrada em contratos, por parte de consumidores, com retalhistas *online*. Essa anomalia é a confiança, ou, melhor dizendo, a falta dela.

22 NEWMAN, Abraham L. e BACH, David, "*Self-Regulatory Trajectories in the Shadow of Public Power : Resolving Digital Dilemmas in Europe and the U.S.",* Governance: An International Journal of Policy, Administration, and Institutions, Vol. 17, No. 3, Wiley-Blackwell, Julho de 2004, pp. 387–413.

4. CONCLUSÃO: SERÃO OS *SMART CONTRACTS* A SOLUÇÃO PARA A CRISE DE CONFIANÇA?

Circunscrita a anomalia à confiança para entrar num contrato *online*, ter-se-á de analisar se os *smart contracts* serão capazes de ser o *new normal* no que toca à elaboração de contratos, enquanto resposta à falta de confiança.

Para alguns, como Matt Byrne, a resposta é afirmativa: "*numerosos futuristas prevêem que os contratos inteligentes, utilizando as emergentes tecnologias do blockchain e menos estritos códigos de programação, irão resultar em contratos sendo escritos como código imutável numa blockchain privada, cantarolando harmoniosamente e auto-executando-se e autorregulando-se*[1]*".*

Para outros, como Kevin Werbach e Nicolas Cornell, a resposta é negativa. Para estes, apesar das características singulares que têm, os contratos inteligentes não colocarão em causa o paradigma actual, representado pela Lei de Contratos em vigor. Para estes autores, "*enquanto os smart contracts podem ir ao encontro dos requisitos doutrinais da Lei dos Contratos, eles servem um propósito fundamentalmente diferente. A Lei de Contratos é uma instituição reparadora. O seu objectivo não é assegurar a execução ex ante, mas para adjudicar as reclamações que surgem ex post. Os contratos inteligentes tornaram ainda mais evidente esta função axiomática da Lei dos Contratos. As necessidades que deram origem à Lei dos Contratos, no entanto, não desaparecem. Se as partes não podem - ou não conseguem - prever, ex ante, todas as possíveis situações que poderão surgir durante a vigência do contrato, o resultado pode divergir da sua intenção inicial convencionada*[2]*".*

Desta forma, coloca-se a questão: será que os contratos inteligentes serão a solução para a crise de confiança endémica na contratação *online*? Indo mais longe, será

1 BYRNE, Matt, "*Do lawyers have a future?"*, Revista *online* "The Lawyer", 20 de Setembro de 2016, disponível em https://www.thelawyer.com/issues/online-september-2016/do-lawyers-have-a-future-2/. Em sentido semelhante mas com soluções que ainda involvem o Estado enquanto decisor, SAVELYEV, Alexander, "*Contract Law 2.0: Smart contracts as the beginning of the end of classic contract law*", Working Paper, National Research University Higher School of Economics, 2016, disponível em SSRN : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241

2 WERBACH, Kevin D. e CORNELL, Nicolas, "Contracts Ex Machina", Duke Law Journal, n.º 67, Duke Law University, Estados Unidos da América, 2017, página 318.

a capacidade dos contratos inteligentes de resolverem, por si, as questões entre as partes, sem a necessidade de terceiros, suficiente para restabelecer a confiança das mesmas para contratar *online*?

A resposta não se afigura simples, tendo em conta que os *smart contracts* não são, ainda, *the new normal.* São (ainda) poucos os advogados capazes de perceber o seu verdadeiro alcance ou funcionamento. Para além disso, a novidade da tecnologia que o fundamenta provoca um misto de estranheza, perplexidade e apreensão, provavelmente motivada pelas dificuldades técnicas que um advogado sentirá para implementar os mesmos. Por outro lado, são as próprias partes que, acostumadas aos contratos de sempre, apresentam alguma resistência à transição, instigada pela ausência de informação, legislação ou regulamentação unânime por parte do legislador que auxilie e favoreça a efectivação massiva dos contratos inteligentes. Ainda, paradoxalmente, na ausência de jurisprudência na matéria a considerar como válidos e eficazes este tipo de contratos, as partes preferem a segurança do que já conhecem, bem como a garantia do conhecimento que as respostas jurisprudenciais já dadas oferecem em caso de incumprimento, numa previsão impossível de ser realizada para quem firma contratos inteligentes. Por último, a regulamentação actual, de que o Regulamento Geral de Protecção de Dados é exemplo, é adversa à rigidez imutável da blockchain, o que deixa dúvidas quanto à longevidade da tecnologia que suporta os *smart contracts*.

Por outro lado, é incontestável que há uma anomalia, que esta permanece válida, e que se traduz na falta de confiança dos consumidores para entrar em contratos *online*. E não há como não olhar para as possibilidades permitidas pelos contratos inteligentes como sendo capazes de assumir papel preponderante no restabelecer da confiança das partes, na certeza de que os contratos inteligentes poderão ajudar a resolver algumas questões que o mundo físico - dividido em países, fronteiras e jurisdições com diferentes entendimentos da Lei - ainda mantém vivas. Como refere Rosalie Abella, Juíza do Supremo Tribunal do Canadá, "*a Internet não tem fronteiras - o seu habitat natural é global*[3]*".*

Conclui-se, desta forma, que nos parece possível que os contratos inteligentes provoquem alterações substanciais na maneira como as partes interagem nos mercados

3 Ver Decisão do Supremo Tribunal do Canadá, Google v. Equustek, 2017 SCC 34, disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do

online. Mas que, enquanto solução para a anomalia detectada, ainda existem muitas interrogações e obstáculos, quer de quem faz os contratos, quer de quem os assina, que terão de ser ultrapassados para que os contratos inteligentes surjam como resposta prática à anomalia. Tal só será possível com uma compreensão dos agentes jurídicos, no seu todo, para as que os contratos inteligentes permitem, bem como a sensibilização das partes para as vantagens dos mesmos. Sem isso, dificilmente os contratos inteligentes terão a utilização intensiva, reiterada e eficaz necessária para gerar a confiança que, também eles, carecem para subsistirem. Porque a falta de confiança que hoje existe em relação à contratação *online,* pode muito bem alastrar-se aos contratos inteligentes. E sem a confiança das partes em contratar através dos contratos inteligentes, a anomalia não só persiste, como aumenta de dimensão.

OPINIÃO

RGPD – REVISITANDO OS DIREITOS INDIVIDUAIS

RUI MANUEL SOARES [1]

1 Senior Consultant and Tutor. Senior Manager | Focus2Comply. E-mail: rui.soares@focus2comply.pt

De alguma forma, estaremos convencidos de que a intenção primacial do RGPD (Regulamento Geral de Proteção de Dados) é fortalecer e unificar a proteção de dados para todos os indivíduos dentro da União Europeia. De um lado, o indivíduo (cidadão europeu ou residente na UE) deverá compreender o cardápio de direitos que lhe assiste. Por outro lado, as entidades que controlem ou processem dados pessoais destes deverão firmar como endereçá-los de acordo com o RGPD.

Apresentam-se estes direitos individuais de forma sintética, bem como pontos a ter em conta para os mesmos, nas iniciativas na sua organização, relativas à proteção de dados para cumprimento do RGPD, que entra em vigor a 25 de Maio de 2018.

Os seguintes direitos individuais são cobertos pelo RGPD:

1. O direito de ser informado

2. O direito de acesso

3. O direito de retificação

4. O direito ao apagamento dos dados

5. O direito à limitação de processamento

6. O direito à portabilidade de dados

7. O direito a oposição

8. Direitos em relação à tomada de decisão ou criação de perfil automatizados.

De um modo sincrético, os direitos dos indivíduos, supra mencionados, incluem dois novos direitos no RGPD, a saber: "Artigo 18 - Direito à restrição de processamento" e "Artigo 20 - Direito à portabilidade de dados", bem como um alargamento, em alguns casos, dos direitos já previstos na Diretiva 95/46 / CE.

1. O direito de ser informado

Este direito assegura transparência pela comunicação de quais são os dados pessoais usados do indivíduo. Uma nota de privacidade é um mecanismo eficaz para esta comunicação. O que e quando informar dependerá de como os dados pessoais foram obtidos.

Notem que as informações fornecidas sobre o processamento de dados pessoais têm de ser claras e sem custo para o indivíduo.

2. O direito de acesso

Os indivíduos têm o direito de verificar a legalidade do modo como os seus dados pessoais são usados e por isso precisam aceder facilmente a estes (e dentro de prazos razoáveis - quando possível, o controlador deverá fornecer acesso remoto a um sistema seguro, que permita acesso direto do indivíduo aos próprios dados pessoais). O considerando 63 fornece mais pormenores sobre este direito. Não descurar que pedidos excessivos podem ser cobrados.

A entidade inquirida tem de fornecer as informações solicitadas sem demora, num prazo inferior a um mês. Para solicitações complexas, a entidade poderá dar a informação em prazo alargado até mais dois meses adicionais, desde que informe do alargamento dentro do primeiro mês após recebimento da solicitação (e explicando o motivo da extensão).

Vejam o exemplo de uma lista de verificação para o tratamento de solicitações de acesso a dados pessoais está disponível no Information Commissioner's Office (ICO) do Reino Unido.

3. O direito de retificação

O titular dos dados tem o direito de obter do responsável pelo tratamento, sem demora injustificada, a retificação de dados pessoais imprecisos que lhe digam respeito.

Tendo em conta a finalidade do tratamento, o titular dos dados tem o direito de ver os seus dados pessoais, que estejam incompletos, devidamente completados, inclusive através da entrega de uma declaração adicional.

Este direito é constante do artigo 16º - Direito à retificação do RGPD, é, ainda, detalhado no considerando 65 - Direito de retificação e apagamento.

4. O direito ao apagamento dos dados

Este direito foi alargado a partir de disposições anteriores. Os controladores têm de apagar dados pessoais se um destes casos for aplicável:

- Quando os dados pessoais já não são necessários em relação à finalidade para a qual foram originalmente recolhidos;
- Quando o indivíduo retira o consentimento;
- Quando o indivíduo objeta ao processamento e não houver interesse legítimo superior para continuar o processamento;
- Os dados pessoais foram processados ilicitamente (ou seja, violando o RGPD);
- Os dados pessoais têm de ser eliminados para cumprir uma obrigação legal;
- Os dados pessoais são processados em relação a oferta de serviços da sociedade da informação a uma criança.

Não obstante, o controlador pode recusar-se a cumprir uma solicitação de eliminação quando os dados pessoais são processados por um dos seguintes motivos:

- Exercício do direito de liberdade de expressão e de informação;
- Cumprimento de uma obrigação legal;
- Realização de uma tarefa de interesse público;

- Exercício de autoridade oficial;

- Para fins de saúde pública de interesse público;

- Com a finalidade de arquivamento de interesse público, pesquisa histórica, pesquisa científica ou fins estatísticos;

- Exercício ou defesa de ações judiciais.

Este direito é relevante, em particular, se a pessoa em causa dera o seu consentimento quando criança, logo não tendo consciência dos riscos envolvidos, e, posteriormente, quer remover os seus dados pessoais, especialmente da Internet (conforme referido no considerando 65). O titular dos dados pode exercer este direito quando adulto. Observar que há alguns casos em que o controlador ainda pode manter algumas informações.

5. O direito à limitação de processamento

Apagar os dados nem sempre é a ação mais adequada. Isto porque mesmo que a finalidade original para o processamento dos dados já não seja aplicável, pode haver uma obrigação legal de manter esses dados pessoais.

Este direito é útil para os próprios controladores, mesmo até nos casos em que os dados são imprecisos ou quando a base legítima do processamento não pode ser imediatamente provada.

O controlador é obrigado a limitar o processamento de dados pessoais se:

- Um indivíduo contesta à exatidão de seus dados pessoais; o processamento tem de ser restringido até que o controlador tenha verificado a exatidão dos dados pessoais;

- Quando o processamento é ilegal e o indivíduo se opõe ao apagamento e solicita limitação;

- Se o controlador já não precisar dos dados pessoais, mas o indivíduo necessita dos dados para estabelecer, exercer ou defender uma causa legal;

- Quando um indivíduo se opõe ao processamento (que era necessário para o desempenho de uma atividade de interesse público ou por interesse legítimo), e a organização está a avaliar se tem base legal legítima superior à do indivíduo.

Alguns métodos para restringir o processamento são apresentados no considerando 67. Por exemplo, pode-se colocar uma marca nos dados pessoais que tenham restrições ao respetivo processamento. Os controladores têm duas obrigações de comunicação:

- O controlador tem de informar os indivíduos afetados antes que a limitação ao processamento seja levantada.

- Se os dados pessoais em consideração tiverem sido divulgados a entidades terceiras, então estas têm de ser informadas sobre a limitação ao tratamento dos dados pessoais (exceto se for impossível ou se fazê-lo implicar esforço desproporcionado).

Há, naturalmente, exceções. O processamento pode ser restrito, mas ainda possível quando:

- O indivíduo consente explicitamente;

- Para estabelecimento, exercício ou defesa de causas legais;

- Para a proteção dos direitos de outra pessoa singular ou coletiva;

- Por razões de interesse público importante da União Europeia ou de um Estado-Membro.

6. O direito à portabilidade de dados

A portabilidade de dados é um novo direito no RGPD. O titular dos dados tem o direito de receber os dados pessoais que forneceu a um controlador. Os dados pessoais devem estar num formato estruturado, comummente usado e legível (A ICO dá como exemplo o formato CVS) e têm o direito de transmitir esses dados para outro controlador, sem constrangimento para esse controlador destinatário.

Este direito aplica-se quando estas duas condições são satisfeitas:

(i). O processamento é realizado por meios automatizados;

(ii). O processamento é baseado no consentimento dado por um indivíduo ou é necessário para o cumprimento de um contrato.

O indivíduo pode solicitar que o controlador envie os dados pessoais diretamente para outra organização (se for tecnicamente exequível). Pese embora, o controlador não tem de adotar ou manter sistemas de processamento tecnicamente compatíveis com outras organizações.

Porém, a portabilidade dos dados não se aplica quando o tratamento dos dados pessoais for necessário para cumprir uma obrigação legal a que o responsável pelo tratamento está sujeito, ou para a execução de uma tarefa realizada de interesse público ou no exercício de uma autoridade oficial do controlador.

7. O direito de oposição

O titular dos dados tem o direito de se opor quando:

- Não há interesse legítimo ou desempenho de uma tarefa no interesse público / exercício de autoridade pública (incluindo perfil), nos termos das alíneas e) ou f) do n.º1, ou do n.º4, ambos, do Art.º 6.º do RGPD - a menos que o responsável pelo tratamento apresente razões imperiosas e legítimas (e convincentes) para que o processamento continue e se sobreponha aos interesses, direitos e liberdades do titular dos dados ou para o estabelecimento, exercício ou defesa de ações judiciais.

- *Marketing* direto (incluindo perfil) - Neste caso, o direito de oposição deve ser explicitamente levado ao conhecimento do titular dos dados e apresentado de forma clara e separada de qualquer outra informação.

- Investigação científica/histórica ou estatística - a menos que o processamento seja necessário para tarefa realizada por razões de interesse público.

Se o processamento de dados for realizado *online*, o controlador tem de disponibilizar uma maneira de os titulares de dados se oporem *online*.

8. Direitos em relação a decisões individuais automatizadas, incluindo definição de perfis

O RGPD inclui a **salvaguarda dos indivíduos contra o risco de que uma decisão potencialmente prejudicial seja tomada sem intervenção humana**. Com o RGPD há agora novas protecções no que respeita à definição de perfis. Em qualquer caso, esse processamento deve estar sujeito a salvaguardas adequadas, que devem:

- Incluir informação específica à pessoa em causa e o direito de obter intervenção humana;

- Expressar o seu ponto de vista para obter uma explicação da decisão tomada após essa avaliação automática;

- Poder de contestar a decisão.

Por fim, visando garantir um **processamento justo e transparente** em relação ao titular dos dados (incluindo prevenir efeitos discriminatórios sobre uma pessoa), o responsável pelo tratamento deve:

- Usar procedimentos matemáticos ou estatísticos para a definição de perfis;

- Implementar medidas técnicas e organizacionais adequadas para assegurar, em concreto, que fatores que originem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado.

Contudo, o **processamento automatizado é permitido se** um destes casos ocorrer:

- É necessário para celebrar ou executar um contrato entre o titular dos dados e um controlador de dados;

- Está autorizado pela legislação da União (ou do Estado-Membro) a que está sujeito o responsável pelo tratamento (que também inclui medidas adequadas para salvaguardar os direitos e liberdades da pessoa em causa e seus interesses legítimos). A autorização referida pode incluir propósitos de monitorização e prevenção de fraude e evasão fiscal;

- O titular dos dados deu o seu consentimento explícito.

As decisões tomadas a partir de criação de perfis não podem basear-se em dados sensíveis (por exemplo, informações raciais, étnicas ou religiosas), a menos que:

- Exista o consentimento explícito do titular dos dados (exceto quando proibido por legislação da União ou pela legislação nacional)

- O processamento é necessário para um interesse público significativo.

AUTORIDADES DE CONTROLO INDEPENDENTES NO (NOVO) REGULAMENTO GERAL (UE) SOBRE A PROTEÇÃO DE DADOS (RGPD): "*THE NEVER NEVER LAND*"?

JOÃO FERREIRA PINTO [1]

1 Advogado. Mestre em Segurança da Informação e Direito do Ciberespaço (IST). Docente Universitário Convidado. Contacto: Jpinto@adcecija.pt

DIREITOS (FUNDAMENTAIS) DA RESERVA DA VIDA PRIVADA E DA PROTEÇÃO DOS DADOS PESSOAIS NO NOVO REGULAMENTO GERAL (UE) SOBRE A PROTEÇÃO DE DADOS (RGPD).

A Europa tem percorrido um longo caminho, após a II Guerra Mundial, na defesa dos Direitos Humanos (Direitos Fundamentais). Entre estes contam-se dois direitos do Homem fundamentais distintos: o Direito à reserva da intimidade e da vida privada e o Direito à proteção de dados pessoais.

Ao longo de décadas surgem textos internacionais de referência sobre Direitos do Homem, como por ex. a Declaração Universal dos Direitos do Homem, da ONU (1948) e a Convenção Europeia dos Direitos do Homem, do Conselho da Europa (1950).

No que diz respeito aos direitos (humanos) da reserva da vida privada e da proteção de dados pessoais, surgem textos "icónicos" como as "Guidelines" da (OCDE) em 1980 e a "Convenção 108" do Conselho da Europa (1981).

Na União Europeia (UE) surge, em 2000, a "Carta dos Direitos Fundamentais da União Europeia" elevada à "categoria jurídica" de Tratado Fundamental/Institutivo da UE em 2009 pelo Tratado de Lisboa (assinado no Mosteiro dos Jerónimos).

A defesa dos Direitos Fundamentais/do Homem consagrados na "Carta", entre os quais o Direito à reserva da vida privada (cfr. art.º 7.º) e o Direito à proteção dos dados pessoais (cfr. art.º 8.º), só é congruente através de uma disciplina jurídica única e igual em todo o espaço da União Europeia.

Com esta perspetiva de "unicidade global" dos Direitos do Homem na UE é proposta, a 25 de Janeiro de 2012, a revisão da legislação europeia sobre proteção de dados pessoais (a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995) através de um instrumento legal único e "forte", o Regulamento Comunitário.

Em 2016, após um longo processo legislativo sujeito a um *lobby* que a Comissária Europeia Viviane Reding, Vice-Presidente da Comissão Europeia, chegou a classificar publicamente como "violento", é finalmente aprovado o Regulamento Geral sobre a Proteção de Dados (RGPD) que entra em vigor em Maio de 2016 e é aplicável a partir de 25 de Maio de 2018 (o 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).

O Regulamento Geral (UE) é uma "lei comunitária" vinculativa em todos os seus elementos, que vigora diretamente na ordem jurídica nacional e possui dois "objectos e objectivos": a defesa dos direitos e as liberdades fundamentais das pessoas singulares, nomeadamente, o direito à proteção dos dados pessoais e a livre circulação desses dados (cfr. art.º 1.º).

Sendo uma única e a mesma "lei" aplicável em todo o espaço da União Europeia - alargada ao Espaço Económico Europeu (EEE) -, o RGPD introduz um sistema inovador de "one stop shop" ou mecanismo de "balcão único"

O balcão único assenta no conceito de Autoridade de Controlo Principal (cfr. art.º 56.º). Isto é, a autoridade de controlo da jurisdição onde se localiza o estabelecimento principal do responsável pelo tratamento ou do subcontratante, que é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço efetuado pelo responsável ou pelo subcontratante.

Do ponto de vista dos "tratamentos transfronteiriços" de dados dentro da UE/EEE (cfr. art.º 4.º, n.º 23), o responsável ou subcontratante passa a ter a possibilidade de se "relacionar" e "prestar contas" apenas a uma (única) Autoridade de Controlo que passa a ser a Principal, em vez de ter de lidar de forma individualizada com cada uma das Autoridades Controlo existentes nas jurisdições dos (atuais) 28 Estados-Membros da UE para onde efetua transferências/tratamentos de dados.

A existência de um Regulamento Geral "único" e o mecanismo do "balcão único" – com vantagens evidentes para os operadores do Mercado Único Digital -, coloca assim

grandes desafios ao sistema institucional de controlo e de proteção de dados pessoais na UE.

Em resposta a este princípio do controlo e aplicação coerentes do Regulamento em toda a União Europeia é redesenhado todo o novo sistema institucional, no RGPD, dotado de novos e poderosos mecanismos de cooperação e coerência entre as diversas Autoridades de Controlo, no qual pontifica um novo Comité Europeu para a Proteção de Dados.

2. SISTEMA INSTITUCIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA LIBERDADE DE CIRCULAÇÃO DOS DADOS NA UNIÃO EUROPEIA.

a) O novo Comité Europeu para a Proteção de Dados (o "Comité")

O novo sistema institucional cria o Comité Europeu para a Proteção de Dados (o "Comité") enquanto organismo da União, dotado de personalidade jurídica.

É composto pelos directores/representantes de cada uma das autoridades de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados (cfr. artigos 68.º a 76.º e Considerandos 139 e 140).

O Comité Europeu para a Proteção de Dados tem como atribuição assegurar a aplicação coerente do Regulamento, sendo dotado de poderes, que pode exercer por iniciativa própria ou a pedido da Comissão, entre os quais os seguintes: controlar e assegurar a correta aplicação do Regulamento; aconselhar a Comissão nas questões relacionadas com a proteção de dados pessoais na União; emitir e examinar a aplicação prática de diretrizes, recomendações e melhores práticas; elaborar diretrizes dirigidas às autoridades de controlo; das diretrizes, recomendações e melhores práticas ; incentivar a elaboração de códigos de conduta e a criação de procedimentos de certificação, de selos e marcas de proteção dos dados; acreditar os organismos de certificação; emitir parecer à Comissão para a avaliação da adequação do nível de proteção num país terceiro ou organização internacional; emitir pareceres relativos aos

projetos de decisão das autoridades de controlo nos termos do procedimento de controlo da coerência e emitir decisões vinculativas; promover a cooperação e o intercâmbio bilateral e plurilateral efetivo de informações e as melhores práticas entre as autoridades de controlo; promover programas de formação comuns e facilitar o intercâmbio de pessoal entre as autoridades de controlo; promover o intercâmbio de conhecimentos e de documentação sobre as práticas e a legislação no domínio da proteção de dados com autoridades de controlo de todo o mundo; emitir pareceres sobre os códigos de conduta elaborados a nível da União; conservar um registo eletrónico, acessível ao público, das decisões tomadas pelas autoridades de controlo e pelos tribunais sobre questões tratadas no âmbito do procedimento de controlo da coerência.

Do ponto de vista da elaboração de diretrizes, recomendações e melhores práticas, o Comité passa a ter um papel mais interventivo, substituindo o papel relevante consultivo desempenhado pelo Grupo de Trabalho do Artigo 29 da Directiva 95/46/CE.

b) Autoridades de Controlo independentes

A nível dos Estados-Membros da UE, a defesa dos direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento de dados e da liberdade de circulação desses dados na União, continua confiada às "Autoridades de Controlo" Independentes com a responsabilidade de zelar pela fiscalização da aplicação coerente do Regulamento (cfr. CAPÍTULO VI, artigos 51.º a 59.º e Considerandos 117 a 132).

Para o efeito, as autoridades de controlo cooperam entre si e com a Comissão, e possuem assento no "Comité".

As autoridades de controlo mantêm um estatuto de independência na prossecução das suas atribuições e no exercício dos poderes atribuídos pelo Regulamento.

Em Portugal a Autoridade de Controlo independente é a Comissão Nacional de Proteção de Dados (CNPD), constituída em 1994.

A CNPD é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República.

Tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.

Possui como atribuições principais: controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais; emitir parecer prévio sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos comunitários ou internacionais relativos ao tratamento de dados pessoais; exercer poderes de investigação e inquérito, podendo para tal aceder aos dados objeto de tratamento; exercer poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, assim como o de proibir temporária ou definitivamente o tratamento de dados pessoais; advertir ou censurar publicamente o responsável do tratamento dos dados, pelo não cumprimento das disposições legais nesta matéria; intervir em processos judiciais no caso de violação da lei de proteção de dados; denunciar ao Ministério Público as infrações penais nesta matéria, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de provas (cfr. artigos 21.º a 31.º da Lei n.º 67/98, de 26 de Outubro, a "Lei de Proteção de Dados Pessoais").

Relativamente à independência e eficácia das autoridades de controlo o Regulamento consagra como requisitos a cumprir pelos Estados-Membros, a obrigatoriedade de fornecer os recursos financeiros e humanos, as instalações e as infraestruturas necessárias ao desempenho eficaz das atribuições das autoridades de controlo, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União (cfr. Considerando 120).

Por outro lado, as autoridades de controlo deverão ter, em cada Estado-Membro, as mesmas funções e poderes efetivos, incluindo poderes de investigação, poderes de correção e de sanção, e poderes consultivos e de autorização, nomeadamente em caso

de reclamação apresentada por pessoas singulares, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, tendo em vista levar as violações ao presente regulamento ao conhecimento das autoridades judiciais e intervir em processos judiciais (cfr. Considerando 129).

c) Cooperação e coerência

São reforçados os poderes das autoridades de controlo independentes que devem prestar-se mutuamente assistência no desempenho das suas funções, por forma a assegurar a execução e aplicação coerentes do Regulamento, e devem, também, participar em operações conjuntas com outras autoridades de controlo (cfr. Considerandos 133 e 134 e artigos 60.º a 62.º)

Por outro lado, para assegurar a aplicação coerente do Regulamento na UE, é criado um procedimento de controlo da coerência e para a cooperação entre as autoridades de controlo que é aplicável: quando uma autoridade de controlo tenciona adotar uma medida que visa produzir efeitos legais em relação a operações de tratamento que afetem substancialmente um número significativo de titulares de dados em vários Estados-Membros; e sempre que uma autoridade de controlo interessada, ou a Comissão, solicitar que tal matéria seja tratada no âmbito do procedimento de controlo da coerência (cfr. Considerandos e artigos 63.º a 67.º).

O procedimento de controlo da coerência passa pela emissão de parecer do Comité sobre a questão concretamente visada constante do projeto de decisão elaborado por uma autoridade de controlo (cfr. art.º 64.º).

Em casos excecionais de urgência na defesa dos direitos e liberdades dos titulares dos dados, a autoridade de controlo interessada pode adotar imediatamente medidas provisórias (válidas até três meses) destinadas a produzir efeitos legais no seu território.

O novo sistema institucional de proteção de dados pessoais e da liberdade de circulação dos dados na União Europeia, terá grandes desafios não só para as autoridades de controlo independentes, mas também para o novo "Comité", dado o

reforço dos direitos dos titulares dos dados no Regulamento e o incremento da liberdade de circulação digital de dados no Mercado único Digital.

Numa perspetiva de assegurar a execução coerente do Regulamento, é um sistema que se encontra dotado dos mecanismos legais à altura do "desafio" que se coloca na proteção dos direitos fundamentais de "segunda geração" iniciada pelo Regulamento Geral de Proteção de Dados (RGPD).