UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

MESTRADO EM DIREITO E PRÁTICA JURÍDICA

DIREITO DA EMPRESA

O Uso de *Big Data Analytics* e o Reflexo nos Negócios Jurídicos à Luz do Regulamento Geral de Proteção de Dados.

Dissertação apresentada ao Programa de Mestrado em Direito e Prática Jurídica da Universidade de Lisboa, como exigência parcial para a obtenção do título de Mestre em Direito da Empresa orientada pelo Professor Dr. Alexandre Sousa Pinheiro.

Vicência Sarkis

2019

Agradecimentos

Qualquer dissertação é norteada por uma trajetória de desafios, dúvidas, tristezas e alegrias, é uma caminhada solitária em que todos os que se propõem a fazer estão dispostos a percorrer esta estrada. Porém, existem pessoas que oferecem um contributo indispensável para encontrar-se a melhor forma de caminhar.

A trilha que foi percorrida só foi possível com o contributo de algumas pessoas indispensáveis, a quem dedico esse projeto de vida e de trabalho.

Em especial ao meu orientador o professor Doutor Alexandre Sousa Pinheiro que é possuidor de notável saber jurídico com grande experiência académica.

Ao professor Doutor Diogo Pereira Duarte quem me apresentou às novas tecnologias e seus desfechos no direito, matéria que domina com grande sabedoria e empenho.

Ao meu maior companheiro de todas as horas que sempre acreditou na minha dedicação e empenho, João.

Aos meus filhos Danilo e Viviane que agradeço pela enorme compreensão, generosidade e alegria em todas as minhas ausências.

Aos meus amigos Rita e Tobias maiores companheiros em todas as horas.

Por fim, o meu profundo e sentido agradecimento a todas as pessoas que contribuíram para a concretização desta dissertação, estimulando-me intelectual e emocionalmente.

"Se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar, o mundo, que certamente não dispensará a máquina, dispensará o jurista. Será o fim do Estado de Direito e a democracia se transformará facilmente em tecnocracia."

Renato Borruso

Resumo

A presente dissertação versa a análise das questões relativas à proteção de dados suscitadas no contexto do Regulamento Geral de Proteção de Dados – RGPD, considerando os dados gerados através do avanço das tecnologias da informação e comunicação, nomeadamente os caracterizados por um grande volume por unidade de tempo, denominados de *Big Data*.

Com a metamorfose digital dos últimos anos, toda a sociedade vive os seus reflexos no quotidiano e o direito é uma das áreas que também se deverá adequar ao cenário *Big Data* estabelecido digitalmente.

Desta forma, serão focados vários aspetos relacionados com o tema, iniciando com as formas de produção de dados, da parte histórica até aos atuais meios sofisticados no que tange tal produção e os pontos importantes para o alcance de uma proteção mais efetiva possível, abordando desde os princípios fundamentais que presidem à proteção daqueles dados, avançando posteriormente para os direitos dos titulares dos dados merecedores da tutela efetiva no momento das relações jurídicas, assim como as novas medidas que o Regulamento Geral de Proteção de Dados apresenta sobre a matéria.

Porém, e porque é também importante salientar que as redes sociais são na sua maioria colaboradoras para a angariação de dados, sejam estruturados ou não, as novas tecnologias ganham grande importância no cenário hodierno.

No que se refere o Consentimento, este ganha importância no RGPD, integrando-o e refletindo na autodeterminação informacional que tem grande papel como meio de reação ao tratamento de dados pessoais.

Por fim, procede-se a uma tentativa de exposição das várias relações sinalagmáticas que são oriundas das relações no ciberespaço e as suas ressalvas.

Descritores: RGPD, tecnologias, redes sociais, consentimento, tratamento de dados pessoais.

Abstract

This dissertation addresses the data protection issues raised in the context of the General Data Protection Regulation (GDPR), considering the data generated through the advancement of information and communication technologies, namely those characterized by a large volume per unit of time, called Big Data.

With the digital metamorphosis of the last years, the whole society lives its reflexes in the daily life and the law is one of the areas that also must adapt to the scene Big Data established digitally. In this way, various aspects related to the theme will be focused, beginning with the data production means through History, to the current sophisticated means regarding this production and the important points to reach a more effective protection possible, considering the fundamental principles that govern the protection of those data, the rights of data subjects that need effective protection at the time of legal relations, as well as the new measures that the General Regulation on Data Protection presents on the subject.

However, and because it is also important to emphasize that social networks are mostly collaborators for data collection, whether structured or not, new technologies are of great importance in today's scenario. Regarding Consent, it gains importance in the GDPR, integrating it and reflecting in the informational self-determination that plays a great role as a reaction to the processing of personal data. Finally, an attempt is made to expose the various syntagmatic relations that arise from relations in cyberspace and its reservations.

Keywords: GDPR, technologies, social networks, consent, personal data treatment.

Índice

Lista de Siglas e Abreviaturas

Art.º – Artigo

RGPD – Regulamento Geral de Proteção de Dados.

RT - Responsável pelo Tratamento

GT29 - Grupo de Trabalho do Artigo 29

CNPD - Comissão Nacional de Proteção de Dados

Conselho - Conselho Europeu para a Proteção de Dados

EPD - Encarregado da Proteção de Dados

IoT - Internet of Things

TEDH- Tribunal Europeu dos Direitos do Homem

CAPÍTULO I – INTRODUÇÃO

O mundo tem passado por diversas mudanças no aspeto tecnológico nos últimos anos. O ser humano nunca assistiu uma evolução e uma disrupção tão acelerada e com mais eficiência, mudando as cadeias de valores existentes. A evolução não é só tecnológica, mas também nos modelos de negócios a que as empresas necessitam se adaptar para que possam continuar à sua existência.

Para alguns especialistas em tecnologia da informação e comunicação, a tendência da sociedade será de uma economia de dados e sociedade de dados, e não mais como é atualmente uma sociedade de informação ou economia do conhecimento (GRELLER, 2012).

A revolução digital nas últimas décadas resultou numa explosão na capacidade de produzir, de armazenar, transmitir e manipular grandes quantidades de dados. Apenas um quarto de toda informação armazenada no mundo, no ano 2000, era em formato digital. Isto significa que a maior parte dos dados estavam em papel ou outras formas analógicas de armazenamento. Em 2013 já se constatava que menos de 2% de toda informação armazenada no mundo não é digital (CUKIER, 2013).

Em todas as áreas pode-se detetar mudanças significativas, como por exemplo os hábitos tecnológicos das pessoas, a forma como as empresas necessitam se adaptar para que possam continuar a realizar os seus negócios, as exigências que o mercado impõe no que tange a agilidade das prestações dos serviços entre outras. A internet vem colaborar com

a sociedade do século XXI, interligando pessoas e dispositivos a qualquer hora e em qualquer lugar por sensores omnipresentes, onde a troca de valores é uma das suas características. Pode-se afirmar, com toda a certeza, que é um momento único da história da civilização humana.

Toda a tecnologia gera informações sobre determinada matéria. Desta forma, é uma ferramenta de muita importância para se estabelecer uma decisão. Os dados que são gerados a cada minuto, por cada pessoa, dão origem ao que se chama *Big Data*, que de forma simplificada pode-se dizer que representa um grande volume de dados.

A matéria em apreço, possui um grau de importância elevado nos dias atuais, devido às mudanças tecnológicas, sociais e consequentemente económicas, pelo que muitas vezes

os métodos tradicionais de tutela das pessoas, tornam-se rapidamente obsoletos quando em comparação com a evolução tecnológica. O legislador ao tempo da promulgação da lei conseguia proteger as pessoas à época da mesma. Atualmente, muitas vezes para se garantir a justa aplicação dos direitos codificados, são necessários fazer novas leis e novas interpretações para que a adaptação à corrida tecnológica seja adequada conforme as funções precípuas do direito.

1.1 Evolução e Conceitos Preliminares

Vai-se agora descrever os primórdios dos meios de organização dos dados das sociedades que ofereceram meios para estabelecer novas conexões entre o conhecimento de gerações em gerações. A escrita é considerada a primeira forma de dados estruturados[1]. Anteriormente estes não existiam sendo os dados representados por marcas, gravações de figuras, rastos de animais, etc. (CALVETE, 1996).

1.2 Evolução Histórica

O mundo encontra-se na Quarta Revolução Industrial[2], onde a revolução tecnológica está marcada por alterações profundas de como as pessoas se relacionam, seja no ambiente de trabalho, lazer, desporto e etc. (SCHWAB, 2009).

Convém, antes de tudo o mais, referir a primeira forma de comunicação, que remota à época anterior à escrita, onde se passava a informação de forma verbal.

A escrita, que foi desenvolvida com o passar dos anos, pode ser considerada como sendo a primeira forma de estrutura da informação, o que permitiu, de uma forma mais

[1] Os dados estruturados são aqueles que possuem como se fosse uma etiqueta, sendo mais facilmente identificável. AKOKA, J., Wattiau, I., & LAOUFI, *N - Research on Big Data- A systematic mapping study*. [Em linha]. [2017]. [Consult. 05 jan. 2019]. Disponível emWWW:<URL:https://www.sciencedirect.com/science/article/abs/pii/S0920548917300211>.

[2] A Primeira Revolução data de entre finais do século XVIII e início do século XIX (criação das máquinas a vapor e o carvão), a Segunda Revolução do meio do século XIX (com a eletricidade) e a Terceira Revolução Industrial da segunda metade do século XX (revolução digital). Segundo o presidente do Fórum Económico Mundial de Davos, a Quarta Revolução Industrial está a decorrer, sendo baseada nas novas tecnologias e integração entre as mesmas, sendo elas, a título exemplificativo: a digitalização, internet das coisas, *blockchain*, *Big Data*, impressão 3D, engenharia genética, inteligência artificial e veículos autônomos. SCHWAB, Klaus - *Word Economic Forum*. [Em linha]. [2015]. [Consult. 21 jan. 2019]. Disponível em WWW:<URL:https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond >.

facilitada, passar para gerações futuras dados importantes da cultura de um povo. Já escreveu Moncada (2014, p. 7):

"Não basta conhecer os problemas; é preciso conhecer também a história deles. O homem é um ser histórico. É mesmo o único ser histórico que se conhece. A história é, mais que uma simples sucessão cronológica de factos e aconteceres coisificados e tornados estranhos ao homem, a própria essência e substância da sua vida espiritual."

Na mesma linha argumentativa histórica, é com muita frequência que se imagina que a comunicação é uma consequência do desenvolvimento dos computadores, quando na verdade o que se constata, é que são os computadores uma consequência da estrutura dessa informação, criada com a evolução dos aparelhos eletrónicos.

A tecnologia, como regra, assim como o surgimento dos computadores, tem uma evolução proeminente derivada de conflitos bélicos. Dificilmente se consegue exprimir uma análise doutrinária de forma mais eloquente do que fez Alexandre Sousa Pinheiro (2015, p. 71) quando escreveu:

"A evolução científica, especialmente sensível após a Segunda Guerra Mundial – a mãe de todas as tecnologias -, teve serias repercussões nas ciências da comunicação. As contingências bélicas obrigaram à descoberta de processos de transmissão de mensagens, e de modelos de linguagem, com um elevado nível de complexidade que, fora do espaço militar, serviriam – primeiramente – ao Estado para desenvolver as, hoje correntes, tecnologias da comunicação. Desempenharam um papel expressivo neste movimento renomados cientistas que participaram no que começaram por ser meros encontros entre especialistas em inteligência artificial, cibernética e comunicação automatizada…"

Com efeito, a evolução tecnológica cujos resultados, anteriormente tinham como destino as necessidades do Estado, hoje encontra-se presente nas casas da maioria das pessoas, que podem dispor da mesma para as mais diversas finalidades. A evolução foi tão marcante e surpreendente que os computadores que eram de um tamanho de um automóvel de médio porte (por exemplo), hoje cabem na palma da mão.

A Internet é a maior rede de comunicação mundial existente atualmente, não há que se duvidar desta informação, para se ter ideia da evolução e do tempo que caiu no hábito das pessoas a nível de comparação[3], vejamos:

-A televisão criada em 1948, demorou 7 anos para alcançar 75% dos lares americanos;

-O telefone criado em 1890, demorou 67 anos;

-O automóvel criado em 1908, demorou 52 anos;

-O aspirador criado em 1913, demorou 48 anos;

-O ar condicionado criado em 1952, demorou 48 anos;

-O rádio comercializado em 1923, demorou 14 anos (PUTNAM, 2000).

Perfunctoriamente, sobre a velocidade da evolução digital, observa-se que em 1969 houve a criação da ARPAnet[4]. Foi nesse ano que se constata a primeira transmissão por rede que ocorreu entre a UCLA[5] e Stanford[6]. Em 1971, após 2 anos, foi criado o primeiro programa de e-mail chamado por SNDMSG, por Ray Tomlinson[7], que era funcionário da Bolt Beranek and Newman (BBN). E que em 1968 foi contratado para concretizar a implementação da ARPANET. No ano de 1982, aparece pela primeira vez a definição do termo, que se conhece atualmente como "internet", ano em que a revista *Time* declara não a pessoa do ano, mas a máquina do ano, o computador.

Observa-se que o lapso temporal transcorrido de 13 anos, atualmente é considerado enorme para a evolução que resultou. Nos últimos 10 anos houve a verdadeira revolução digital, com a criação e desenvolvimento de plataformas digitais, mais especificamente as redes sociais, como a Myspace e Orkut (que já não existem), Facebook, Twitter, WhatsApp, entre outros. Possui o poder de permitir interagir com outras pessoas com

[3] Dados recolhidos por Putnam, que foram publicados na *Economic History Review*.
[4] ARPANET - *Advanced Research Projects Agency Network* foi uma rede operacional que pertencia ao Departamento de Defesa americano, é considerada a primeira rede operacional de computadores, sendo o precursor da internet. Sua finalidade era exclusivamente para fins militares. [Em linha]. [2014], [Consult. 28 nov. 2018]. Disponível em WWW:<URL:https://www.britannica.com/topic/ARPANET>.
[5] Universidade da Califórnia em Los Angeles.
[6] Universidade Stanford (Stanford University - *Leland Stanford Junior University*) é uma universidade de pesquisa privada situada na Califórnia, sendo considerada uma das instituições mais prestigiadas do mundo.
[7] TOMLINSON, Raymond - *Official Biography*: Raymond Tomlinson. [Em linha]. [2018]. [Consult. 20 nov. 2018]. Disponível em WWW:<URL:https://www.internethalloffame.org/official-biography-raymond-tomlinson>.

textos, vídeos, imagens, músicas, participar de grupos de discussão de variados assuntos, etc.

A evolução digital favoreceu uma evolução social. Como exemplo pode-se citar as "revoluções do Twitter"[8] que em alguns países como a Tunísia e o Egipto levaram o uso de redes sociais, com a finalidade de organizar, comunicar e, por fim, dar início a campanhas de desobediência civil e ações de rua.

A "Revolução Verde" iraniana em 2009, foi seguida pelos media ocidentais por YouTube e Twitter, que assim auxiliaram e motivaram às pessoas a lutarem por mudanças. Todos os setores sofreram influência da referida revolução.

No mercado de trabalho o *Mckinsey Global Institute* apresentou uma pesquisa, em que concluiu que cerca de 50% de todas as tarefas realizadas por pessoas, poderiam ser automatizadas a partir das tecnologias já existente e disponíveis em 2016[9], nos EUA, existe o *Contract Intelligence* – COIN, que é um sistema de *machine learning*[10] que possui como objetivo a interpretação de acordos de empréstimo comercial e possui a capacidade de realizar análises de acordos na área financeira do banco norte-americano: JP Morgan Chase & Co.. Sendo averiguado que a referida ferramenta, substitui o trabalho de 360 mil horas ao ano de um advogado, também possui como especial característica a diminuição de equívocos na elaboração de concessão de serviços de empréstimo que são originários por erro humano (GALEON e HOUSER, 2017). Ainda no mercado de trabalho não se pode ignorar que são em muitos aspetos sentido o reflexo do desenvolvimento tecnológico, como nos casos dos *chatbot*[11], em especial o *chatbot DoNotPay* que funciona no Reino Unido e em Nova Iorque, que realiza contestações de

---

[8] PAPIC, Marko e NOONAM, Sean - *Social Media as a Tool for Protest***.** [Em linha]. [2011], [Consult. 2 dez. 2018]. Disponível em WWW:<URL: https:<//worldview.stratfor.com/article/social-media-tool-protest>.

[9] MANYIKA, James - *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation***.** [Em linha]. [2017]. [Consult. 3 mai. 2018]. Disponível em WWW:<URL:https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.ashx>.

[10] Segundo definição de SAS o significado mais conhecido seria assim definido: aprendizado de uma máquina, que é um método que analisa os dados de forma automatizada, constrói modelos analíticos. Pode-se considerar ser uma das raízes da inteligência artificial que se baseia na ideia que os sistemas podem aprender com dados, identificar padrões e tomar decisões com o mínimo de intervenção humana. SAS - Evolução do *machine learning*. [Em linha]. [2018]. [Consult. 16 jan. 2019]. Disponível em WWW:<URL:https://www.sas.com/pt_br/insights/analytics/machine-learning.html>.

[11] Criado pelo programador Joshua Browder foi colocado no mercado em 2016, é um programa robotizado que consegue dar respostas às questões colocadas pelas pessoas com grande precisão. VALE. S. - Inteligência Artificial & Redes Sociais: notas sobre um *bot* que odiava humanos. **Revista Interdisciplinar UVA**. Rio de Janeiro: Áquila, 2016.

multas de trânsito oriunda de estacionamento proibido, por ser uma tarefa pouco complexa e com muito trabalho o referido robô é o mais utilizado (SOUZA, 2016).
Em virtude dos factos apresentados, nota-se uma grande revolução tecnológica que ganhou impulso nos últimos anos, e com tendência a ser mais acelerada nos próximos. Concordando com a afirmação onde "Tudo flui, nada permanece, a mudança das coisas é constante e eterna" (Heráclito de Éfeso, 535 a.C.). O computador desde a sua criação, tem utilidade para executar tarefas determinadas pelas pessoas é nesse aspeto que se deve analisar as novas tecnologias e o reflexo no direito (LOVELACE, 1843).

A evolução tecnológica da última década é tão grande, que as máquinas dotadas com Inteligência artificial[12] passaram a realizar tarefas dantes exclusivas das pessoas. Passaram a possuir características de autonomia e cognição, sendo a capacidade de tomar decisões uma característica marcante, com origem na natureza tecnológica que é variável segundo a sofisticação da sua realização (AFFAIRS, 2016, p. 5).

1.3 Finalidades e Conceito de *Big Data*

A rede digital é responsável pela realização de grande parte dos negócios do mundo segundo Kotler e Armstrong (2007, p. 17). Partindo desta afirmação, de forma hodierna, as novas tecnologias são usadas pelas pessoas de forma natural, e com o passar dos anos, nota-se um certo grau de exigência, pelos utilizadores, no que toca a agilidade dos serviços, seja para fazer compras, vendas, pesquisas ou negócios no geral. Este fenómeno é o resultado da popularização da internet.

Tais avanços tecnológicos possuem como motivação as gerações *Millennials*[13] e *Digital Natives*[14], que se mostram pessoas exigentes em relação a rapidez com que os negócios são realizados, apresentam uma preferência na realização de negócio jurídico em linha, em especial o comércio eletrónico[15], fruto de um mundo globalizado e interligado e muito

[12] A Inteligência Artificial (IA) é de difícil definição em braves palavras, contudo, pode-se sintetizar quando se define na atualidade, que há pelo menos três sentidos de "IA" envolvidos: "- Um sistema de computador que se comporta exatamente como uma mente humana; - Um sistema de computador que resolve certos problemas anteriormente solucionáveis apenas pela mente humana e - Um sistema de computador com as mesmas funções cognitivas que a mente humana". 01010 *Informatoin - Conceptions of Artificial Intelligence and Singularity*. [Em linha]. [2018]. [Consult. 22 ago. 2018]. Disponível em WWW:<URL:https://www.mdpi.com/2078-2489/9/4/79/htm>.
[13] Pessoas que nasceram entre 1980 e 1996.
[14] Pessoas que nasceram na era digital acostumadas com a tecnologia avançada.
[15] A definição de comércio eletrônico pode ser assim definida: *"El comercio eletrónico realizado a través de diversos médios eletrónicos y principalmente por internet, se presenta como un área de notable*

comumente chamado de sociedade da informação. Também se observa uma dependência, dessas gerações, aos meios tecnológicos levando a uma mudança de paradigma nas organizações.

O *Big Data* é mais uma dessas mudanças, sendo constituída pelos dados massivos que têm como fonte principal a internet. O utilizador em linha inevitavelmente deixa uma pegada digital, ninguém consegue desaparecer de forma definitiva das grelhas digitais segundo Furtado (2012, p.144), pelos diversos dispositivos que utiliza como: computadores, telemóveis (em especial os *smartphones*), TV *streams*[16], sensores interligados, tablets, relógios (*smartwatch*), etc. Os dados são gerados pelos utilizadores de motores de busca em linha, histórico de pesquisa na *web*, programas de computador, *apps*[17], *downloads*, *e-mails*, *chats*, visualização de vídeos e imagens nas *URLs*, cliques em rede sociais, gestão de conteúdos, perfis criados pelo próprio, para além de registos de localização (como o GPS) entre outros meios. *Big Data* é definido como uma grande pesquisa que representa uma mudança na escala e no escopo do conhecimento sobre um determinado fenómeno (AXELSSON e SCHROEDER, 2014).

Como resultado dessa exposição *online*, muitas organizações empresariais procuram realizar minerações, por exemplo: nas redes sociais como o Facebook, para identificar pessoas que apresentam elevados riscos para o insucesso de cumprimento de contratos jurídicos, conforme o tipo de publicação de cada pessoa em linha. O algoritmo[18]

---

expansión, fenómeno sobre el que existe uma profusa información que nos exime de mayores comentários. El comercio eletrónico tiene fuertes incentivos económicos: una reducción de costos administrativos e impositivos, el acortamiento del processo de distribuición e intermediación, la posibilidad de operar durante todo el dia; la superación de las barreras nacionales; el aumento de la celeridad en las transacciones". LORENZETTI, Ricardo Luís - Informática, *ciberlaw y e-commerce*. **Revista de Direito do Consumidor**. São Paulo: Revista dos Tribunais. n. 36. Out./nov. 2000.

[16] TV *streams* é a possibilidade de assistir conteúdo da televisão nos dispositivos (iOS ou Android), podendo sincronizar canais de TV, funciona em vários formatos (m3u8, mp4, mkv, 3gp, mpv, entre outros) e possui como característica a facilidade de utilização.

[17] Segundo o dicionário Priberam a definição de *APP*: Programa informático que visa facilitar a realização de uma tarefa num computador ou num dispositivo móvel - APLICAÇÃO. "App". Dicionário Priberam – Definição de *APP*. [Em linha]. [2018]. [Consult. 05 out. 2018]. Disponível em WWW:<URL:https://www.priberam.pt/dlpo/app>.

[18]O conceito de algoritmo na matemática é algo que permite resolver um problema. A princípio, na programação também, mas de outra forma. O algoritmo é uma ferramenta que realiza uma tarefa em programação, com o advento de novos projetos se faz necessário desenvolver projetos diferentes para conseguir desenvolver problemas novos, como se fosse um algoritmo gigante. Isso acontece porque todas as tarefas no computador são baseadas em algoritmos. Importante salientar que não é uma pessoa que vai executar o que está sendo descrito, e sim, uma máquina. De forma mais simplificada pode-se dizer que algoritmo é constituído por várias funções que processam dados com o objetivo de extrair informações dos mesmos. STEELE, Brian; CHANDLER, Jonh; REDDY, Swarna - ***Algorithms for Data Science***. Suíça: Springer, 2016, p.12.

EdgeRank[19] determina qual será o alcance das publicações baseado no histórico de publicação; faz um critério de avaliação de tudo o que foi publicado no perfil e o impacto sobre a audiência; faz uma seleção do que deve ou não ser exibido. Cada *post* recebe uma pontuação e assim, determina o grau de exposição, a imitar o algoritmo do google o PageRank que tem a mesma finalidade.

Importante salientar que a internet não é a única fonte de *Big Data*. Os dados podem ser recolhidos, gerados e introduzidos por dispositivos sem necessariamente ligação direta à internet. Como exemplo:

-As câmaras de videovigilância;

-Portagens eletrónicas (como a Via Verde) [20];

-Cartões de clientes de supermercados (que incentivam o uso oferecendo promoções);

-O cartão dos transportes públicos;

-O GPS;

- O Sistema PAYT[21] - *"Pay-as-You-Throw"* - em Cascais;

Entre outos meios que não necessariamente precisam estar conectados.

As fases seguintes, que relevam para o escopo do referido trabalho, estão direcionadas para uma análise hodierna do uso das novas tecnologias, e os interesses gerais sobre a recolha, armazenamento e disseminação de grandes volumes de dados que surgiram principalmente com a internet, que resultaram no fenómeno chamado de *Big Data*[22].

---

[19] VALLE, Alberto - O que é EdgeRank do Facebook e qual sua importância. [Em linha]. [2018]. [Consult. 16 jan. 2019]. Disponível em WWW:<URL:https://www.academiadomarketing.com.br/o-que-e-edgerank/>.

[20] A Via Verde é um sistema de portagem eletrónica utilizado em Portugal, que é originário da Universidade de Aveiro, é uma tecnologia que está presente nas autoestradas do país, parques de estacionamento e pontes.

[21] É um projeto piloto chamado waste4Think, que tem como finalidade a implementação de um sistema PAYT coletivo, baseado num modelo de gestão de resíduos mais eficiente. Fazendo uso de aplicações para smartphone, tablet, jogos, plataforma de monitorização ambiental do PAYT e como prémio o processo de gratificação, onde as famílias que alcançam objetivos definidos, ganham benefícios em serviços municipais de forma gratuita, como por exemplo: parques, bilhetes, aluguer de bicicletas entre outros. O projeto acontece da seguinte forma: cada pessoa possui uma chave magnética, que recolhe todos os dados, armazenando a quantidade de vezes que se joga fora determinado tipo de resíduos. Assim, com a monitorização desses dados, se pode comparar com os demais países europeus, que também participam deste projeto. Waste 4 Think Cascais - *Pay-as-you-throw*. [Em linha]. [2017]. [Consult. 3 nov. 2018]. Disponível em WWW:<URL:https://ambiente.cascais.pt/pt/projetos/waste-4-think-cascais>.

[22] O termo *Big Data* não é usado somente na constatação da existência de um conjunto de dados de grande tamanho; também pode-se usar para se referir as tecnologias e todo o processo de recolha, armazenamento, tratamento e análise desses grandes volumes de dados. LEAL, Ana Alves in CORDEIRO, António

O conceito de *Big Data* é definido como sendo o conjunto de informações que possuem uma escala muito grande, que excede a capacidade ou mesmo impossibilita a utilização dos *softwares* tradicionais de recolha, armazenamento, gestão e análise de dados (LEAL, 2017, p. 80). Também pode ser definido o *Big Data* como um conjunto de informações, dados estruturados, semiestruturados e não estruturados, que são recolhidos de diversas fontes (AKOKA e LAOUFI, 2017). Em síntese, o *Big Data* é um termo que é utilizado aos conjuntos de dados que possuem grande dimensão e que estão além das ferramentas usuais de *software* que são usados para capturar, gerir e processar dados que processam dados em um período tolerável segundo Furtado (2012, p. 135).

Segundo o Grupo de Trabalho do Artigo 29 (doravante GT29), os dados em larga escala são dados que apresentam um volume acentuado, extensão avantajada e prolongado, como exemplo: o registo das atividades de um hospital em relação aos doentes[23], os passageiros que utilizam os transportes públicos ao utilizar o passe, os dados de geolocalização de clientes de uma rede de restauração, a serem utilizados por um subcontratante[24] para fins estatísticos entre outros.

A tecnologia *Big Data* segundo Manuel David Masseno (2018):

*"*Em termos simples, a *Big Data* resulta de confluência de três avanços tecnológicos de origem diferente, mas que se reforçam entre si. Designadamente, da computação em nuvem, a qual passou a possibilitar o armazenamento de volumes crescentes de dados, com disponibilidade permanente e uma fiabilidade assegurada pela redundância, tudo isto com custos cada vez menores; a que juntaram as comunicações de banda muito larga, em fibra ótica ponto, com velocidades de acesso tais que deixou de ser necessário manter centro de dados próprios, igualmente com custos decrescentes; incorporando-se a ambas, a criação de algoritmos de análise assentes em inteligência artificial, mais do que em força bruta computacional, ainda que distribuída, veio acrescentar a viabilidade de gerir pacotes cada vez maiores de dados, em tempo real. Finalmente, a proliferação de sensores interligados, a que se tem dado o nome de internet das coisas, ou de tudo, veio multiplicar a informação disponível, a qual respeita sempre e em definitiva aos cidadãos-consumidores".

Menezes; OLIVEIRA Ana Perestrelo e DUARTE Diogo Pereira – ***FinTech*- Desafios da Tecnologia Financeira**. Coimbra: Almedina, 2017.

[23] Exemplos recomendados pelo Grupo de Trabalho do Artigo 29.º - Orientações sobre os encarregados da proteção de dados (EPD) (WP 243 rev.01). p. 10. [Em linha]. [2016]. [Consult. 5 dez. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf>.

[24] Art.º 4.º, n. º 8 do RGPD. Define como subcontratante a pessoa ou o organismo que trata os dados por conta do responsável pelo tratamento.

Com efeito, pode-se afirmar que a tecnologia do *Big Data* é uma consequência de várias tecnologias, com efeito cascata. Sendo o resultado, e as diferentes tecnologias sendo um meio ou caminho. A grande questão é como esta imensa e crescente quantidade de dados gerados a cada minuto será usado para gerar conhecimento e benefícios concretos e quem colherá esses frutos (NEWELL e MARABELLI, 2015; SAMARAJIVA e LOKANATHAN, 2016).

1.4 Vantagens da Utilização de *Big Data*

Em tema de novas tecnologias, é importante salientar que as organizações estão sendo sobrecarregadas com grandes volumes de dados, orientadas para analisar as preferências dos utilizadores, os dados são em escala planetária em que todas as pessoas possuem a capacidade de gerar informações através de vários dispositivos eletrónicos muito comuns atualmente.

O aumento do domínio do conhecimento não melhora apenas os produtos, mas também é uma fonte para decisões estratégicas, com o intuito de alcançar maiores benefícios económico-financeiros. É utilizado técnicas de persuasão das pessoas com base no conhecimento do comportamento e hábitos *online*.

As vantagens podem ser classificadas da seguinte forma:

-Satisfação do Cliente;

-Recolha de dados de variadas fontes;

-Elevada quantidade de dados produzidos;

-Maior Estabilidade dos sistemas;

-Transparência nas relações;

-Capacidade analítica melhorada;

-Redução dos riscos nas relações jurídicas e

-Tomada de decisão mais segura (LEE, 2017).

Pode-se dizer que também é vantagem quando a utilização dos dados está direcionada para melhorar a venda de produtos ou serviços, direcionar esforços de marketing, realizar mudanças de melhoria de produtos, coletando dados valiosos de clientes. Também são

usados para detetar definições de perfis[25] [26] [27] para a realização de contratos de risco (principalmente as seguradoras), definições de perfis para ofertas de produtos e serviços. Sendo a informação verdadeira, estes processos podem permitir prever preferências futuras, e poderão ter como consequência a discriminação de determinados perfis. O perfil demasiado detalhado pode fomentar discriminação[28] em relação ao mesmo, como exemplo, pessoas que não praticam atividades desportivas serem consideradas de maior risco para a realização de contrato de seguro saúde.

A finalidade que se almeja tem como objetivo a publicidade de produtos e serviços que podem colaborar para a celebração de contratos e angariação de clientes ou a execução e prossecução de contratos já efetivados. A matéria, sobre a publicidade, não é novidade no mercado, remonta ao ano de 1649 (data que alguns autores divergem) quando o primeiro anúncio foi vinculado pelo jornal *Impartial Intelligencer* na Inglaterra (CHAVES, 2005). O objetivo antes e atual é o mesmo: a venda de produtos e serviços, a diferença é que atualmente se recorre as novas tecnologias e se consegue a venda aliada a dois aspetos importantes: aumento da eficiência (agilidade) e economias de recursos (uso de plataformas, armazenamento em nuvens entre outros).

[25] Art.º 4.º, n.º 4 do RGPD sendo a definição de perfil composta de três elementos: deve ser uma forma de tratamento automatizada, efetuada sobre dados pessoais e o seu objetivo deve se avaliar os aspetos pessoais de uma pessoa singular.

[26] Segundo o GT29: "A definição de perfis tem de implicar alguma forma de tratamento automatizado – ainda que uma intervenção humana não exclua necessariamente a ação do âmbito da definição. O processo de definição de perfis pode implicar um conjunto de deduções estatísticas. É frequentemente utilizado para efetuar previsões sobre as pessoas, recorrendo a dados provenientes de várias fontes para inferir algo sobre uma pessoa, com base nas qualidades de outras pessoas que, estatisticamente, parecem semelhantes." Sendo assim, pode ser criado um perfil de uma pessoa que não tenha passado por nenhuma avaliação nos seus dados pessoais, somente por comparação (*online*) de gestos e atitudes semelhantes as demais pessoas. Grupo de Trabalho do Artigo 29.º - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 (WP251rev.01). [Em linha]. [2017]. [Consult. 2 nov. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf >.

[27] A definição de perfil é o resultado de um processo de busca de conhecimento, como característica, da automatização atual, de padrões provenientes dos dados armazenados, envolvendo diferentes tecnologias, que quando é submetido a interpretação do comportamento, possuem a capacidade de identificar um ser humano ou sujeito não-humano e os hábitos. HILDEBRANDT, Mireille – ***Profiling and the Identity of the European Citizen***. Suíça: Springer Science, 2008, p. 303–344.

[28] As práticas discriminatórias devem ser combatidas, já foi debatido a questão em alguns momentos e deve ser sempre questionada quando houverem indícios de prática discriminatória, esta depende de conduta ou ato (que pode ser ação ou omissão), que resulta em violação de direitos que seja baseado na raça, sexo, idade, estado civil, deficiência física ou mental, opção religiosa e outros. (Acórdão Olsson v. Sweden, do TEDH n.º 10.465/83, de 24/03/1989). As práticas discriminatórias deram origem as listas negras de pessoas indesejáveis que praticaram factos reprováveis socialmente, assim são repudiadas para a realização contratual de negócio jurídico.

As organizações que se destacam como intervenientes em *Big Data* são a IBM, SAP, Oracle, HPE, Palantir, Splunk, Accenture e Dell. A IBM investiu em *Big Data Analytics* desde 2005, e em 2014 concluiu cerca de 40.000 contratos de análise de dados[29].

Diante do cenário em linha atual, faz-se importante saber que, o legislador e o aplicador do direito atentem-se aos novos desafios. O futuro seguirá de forma a desenvolver ainda mais as tecnologias, com mais agilidade e de forma vertiginosa nos anos seguintes, e o direito tem como desafio a adaptação a essas novas realidades, para que possa continuar a tutelar bens jurídicos.

O aumento da produção de dados, que são gerados por cada pessoa, tem como principais responsáveis um conjunto de novas tecnologias. Destacam-se a utilização das redes sociais (que se vale do uso da inteligência artificial), a *IoT*[30] e a computação em nuvem. Com o advento dos *smartphones*, *tablets*, dispositivos como sensores interligados[31], *smartwatch* entre outros, os dados podem ser gerados a partir de qualquer lugar, e possuir um volume que ultrapassa a capacidade de processamento das tradicionais arquiteturas de armazenamento de dados (como exemplo RDBMS *relational database management system*), e ainda sem custo para os utilizadores.

O que espoletou a tecnologia *Big Data*, aconteceu com a publicação de Jeffrey Dean[32] e Sanjay Ghemawat[33] (2008) no USENIX *Association* no 6º Simpósio sobre Projeto e

---

[29] *The University of Edinburgh - Big Data - Global Strategic Business Report - Leading Players Are IBM, SAP, Oracle, HPE, Palantir, Splunk, Accenture, Del' PR Newswire*. [Em linha]. [2016]. [Consult. 29 set. 2018]. Disponível em WWW:<URL:https://www.ed.ac.uk/ >.

[30] *IoT* é A Internet das Coisas (*IoT – Internet of Things*) "compreende todos os aparelhos e objetos que se encontram habilitados a estarem permanentemente ligados à Internet, sendo capazes de se identificar na rede e de comunicar entre si. Podem ter o seu estado alterado através daquele meio, com ou sem o envolvimento ativo do ser humanos e têm capacidade para recolher uma vasta quantidade de informação sobre os que o rodeia. A Internet Society define o IoT em sentido amplo como "a extensão da conectividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores". CNCS- Centro Nacional de Cibersegurança Portugal - A Internet das Coisas (*IoT – Internet of Things*). [Em linha]. [2017]. [Consult. 29 ago. 2018]. Disponível em WWW:<URL:https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/ >.

[31] São sistemas de dispositivos que são interligados entre objetos, animais ou pessoas e que possuem um identificador único que têm a capacidade de transferir e se comunicar através de uma rede *on line* sem que seja necessária alguma interação humana entre os objetos. TechTarget - *internet of things* (*IoT*). [Em linha]. [2017]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>.

[32] Dean tem como carreira a ciência da computação, nasceu nos EUA e engenheiro de *software*. Atualmente é o líder do Google.ai, divisão de inteligência artificial do Google. DEAN, Jeffrey Adgate – Biografia de Jeffrey Dean. [Em linha]. [2016]. [Consult. 3 jan. 2019]. Disponível em WWW:<URL:https://ai.google/research/people/jeff >.

[33] Sua origem: indiano-americano, que trabalha com ciência da computação, é engenheiro de *software*. Atualmente, ele é membro sênior do Google no grupo de infraestrutura de sistemas. Ghemawat trabalha com estreita colaboração com Jeff Dean, como exemplo, o modelo de processamento de grandes dados *MapReduce*, o *Google File System* e os bancos de dados *Bigtable e Spanner*. A Wired, que é uma revista

Implementação de Sistemas Operacionais, que apresentavam um modo de programação chamado *Map-Reduce*[34], que finalmente conseguia processar grandes volumes de dados.

Como característica de tal tecnologia, pode-se observar que nos anos 2000, o analista Doug Laney[35] articulou a definição de *Big Data* em três Vs que são o Volume, a Velocidade e a Variedade.

No crescimento de Volume de dados, encontram-se as empresas que coletam dados de diversas fontes, incluindo as transações financeiras (a Bolsa de Valores de Nova York gera mais de um *terabyte*[36] por dia de dados)[37], redes sociais (entre elas o Youtube, Facebook, WhatsApp, Snapchat, Musical.ly entre outras) e informações de sensores ou dados transmitidos de máquina para máquina (*IoT*). A quantidade de dados criados e armazenados no mundo é quase incalculável, e apenas continua a crescer, pode-se afirmar que atualmente está na casa dos *exabytes*[38].

Na questão da Velocidade, os dados que são transmitidos, devem ser tratados em tempo ágil e hábil. Sensores e medições inteligentes estão impulsionando a necessidade de lidar com fluxos de dados praticamente em tempo real. Os dados são gerados em cada segundo e apresentam-se em constante mutação.

---

norte-americana voltada para a tecnologia, descreveu-o como um dos "engenheiros de *software* mais importantes da era da internet". GHEMAWAT, Sanjay - Biografia de Sanjay Ghemawat. [Em linha]. [2016]. [Consult. 3 jan. 2019]. Disponível em WWW:<URL:https://ai.google/research/people/SanjayGhemawat>.

[34] Segundo Dean: "O MapReduce é um modelo de programação e uma implementação associada para processar e gerar grandes conjuntos de dados que são passíveis de uma ampla variedade de tarefas do mundo real". DEAN, Jeffrey e GHEMAWAT, Sanjay - *MapReduce: A Flexible Data Processing Tool*. [Em linha]. [2010]. [Consult. 19 jan. 2019]. Disponível em WWW:<URL:https://cacm.acm.org/magazines/2010/1/55744-mapreduce-a-flexible-data-processing-tool/fulltext?mobile=false>.

[35] Trabalha como vice-presidente e analista da equipe de pesquisa de *data officer* da Gartner. Aborda a estratégia de dados, forma de economia de informação, inovação de informações, casos de uso de *big data* e análise, monetização de dados, dados abertos, estruturas organizacionais para gerenciamento de dados e equipes analíticas. LANEY, Doug – Biografia de Doug Laney. [Em linha]. [2017]. [Consult. 29 ago. 2018]. Disponível em WWW:<URL:https://www.gartner.com/analyst/40872/Douglas-Laney >.

[36] Sendo 1 *terabyte* 1 000 000 000 000 *bytes*, como exemplo pode-se citar que seria o equivalente a 50 000 árvores que foram transformadas em papel ou 1000 exemplares da *Encyclopedia Britannica.* FURTADO, José Afonso – **Uma cultura da Informação para o Universo Digital**. Lisboa: Fundação Francisco Manuel dos Santos, 2012.

[37] PWC - *Where Have You Been All My Life? How the Financial Services Industry Can Unlock the Value in Big Data.* [Em linha]. [2013]. [Consult. 27 ago. 2018]. Disponível em WWW:<URL:https://www.pwc.com/us/en/industries/financial-services/library/viewpoints/unlocking-big-data-value.html>.

[38] *Exabyte* é uma unidade de medida para armazenamento de dados e equivale a 1 quintilhão de *bytes*. Como exemplo, 1 *exabyte* é o equivalente a 10 000 milhões de exemplares da revista *The Economist.* FURTADO, José Afonso – **Uma cultura da Informação para o Universo Digital**. Lisboa: Fundação Francisco Manuel dos Santos, 2012.

Na Variedade, os dados são recolhidos em diversos formatos como estruturados (numéricos, alfanuméricos, em data bases tradicionais) e não-estruturados (e-mail, vídeo, documentos de texto, áudio, transações financeiras entre outros).

Os dados a partir do *Big Data* trazem um conhecimento derivado que vem claramente favorecer as grandes empresas e os governos, que desta forma passam a realizar análises (por isso chama-se *analytics*) com o auxílio da inteligência artificial, a qual por sua vez utiliza algoritmos.

Há ainda mais potencial para extrair *insights*[39] importantes e aproveitáveis dessas informações, embora apenas uma pequena percentagem dos dados sejam analisáveis com satisfação. Porém, tal já é o suficiente para as empresas oferecerem produtos e serviços de forma personalizada para as pessoas.

Pode-se concluir que a tecnologia do *Big Data* se apresenta como um recurso a ser utilizado pelas empresas, que permite uma oferta de produtos e serviços mais especializados e com ofertas mais bem-adaptada às necessidades das pessoas. Também se conclui que possui como objetivo descobrir e analisar perfis para ponderar a possibilidade de realização de contratos que tenham efeitos jurídicos, sendo uma ferramenta de auxílio, para fomentar o mercado. O preço que se paga diante tanta automatização facilitadora, é sem dúvida a fragilidade que os dados pessoais sofrem no que tange o tratamento dos mesmos, a diminuição da proteção de dados pessoais é o preço que se tem a pagar pela procura da conveniência de realização de transações no ciberespaço.

1.5 A Coleta de Dados Omnipresente

A sociedade vive num mundo de coleta de dados quase omnipresente, resultando numa crescente fusão de dados, entre os dados que nascem digitalmente e são usados digitalmente e os que são a digitalização do mundo físico para o digital[40].

Atualmente o próprio utilizador em linha "ajuda" na orientação de alguns conteúdos que são produzidos minuto a minuto, com os chamados *Tags*, num processo chamado

[39] Palavra inglesa muito utilizada atualmente na literatura de novas tecnologias, significa compreensão, perceção ou revelação repentina. Dicionário Priberam – pesquisa da palavra *insights.* [Em linha]. [2018]. [Consult. 8 ago. 2018]. Disponível em WWW:<URL:https://dicionario.priberam.org/insight>.

[40] DIAS, Valéria - Automação Rompe Limites entre Digital, Físico e Biológico. USP. [Em linha]. [2018]. [Consult. 4 jan. 2019]. Disponível em WWW:<URL:https://jornal.usp.br/tecnologia/4a-revolucao-industrial-rompe-limites-entre-digital-fisico-e-biologico/ >.

tagging[41]. Neste, o próprio utilizador classifica a publicação com palavras chaves de forma autónoma e livre, conseguindo agrupar o conteúdo produzido de forma independente e não confundindo com à *URL* (TRANT, 2008).

Desta forma, a coleta de dados na atualidade é realizada em quase todos os pontos em que uma pessoa se encontra conectada e em todo lugar. Mesmo em casa, através de um *smartphone*, que possui aplicativos que estão ligados a uma conexão em linha, seja para o controlo da temperatura de casa, pelo envio da leitura diretamente para o *smartphone*, que por sua vez permite realizar o controlo remotamente direto ao ar condicionado, ou mesmo no sistema que permite controlar a televisão também através do *smartphone*. A coleta de dados existe em todo o lado em que há conexão, como exemplo também de recolha omnipresente se pode citar a questão do varejo (no Brasil) realizado através da *App* mCommerce[42], que são as compras feitas exclusivamente pelos dispositivos móveis em especial os *smartphones*, que facilita a compra de produtos economizando tempo e esforço. A *App* possui cerca de 50 milhões de utilizadores brasileiros, sendo o segundo maior do mundo, só perde para os EUA. A característica principal é que quase não existe intermediadores na relação, e os produtos que foram comprados são compartilhados em linha o que facilita descobrir quais produtos foram adquiridos e a quantidade, toda informação é gerada e compartilhada no ato da compra *online*.

1.6 A Análise Descritiva, Preditiva e Prescritiva

Somente com a análise de dados pode-se aspirar ter conhecimento de como funciona o *Big Data*, ainda que sumariamente. São três as formas dessa análise: análise descritiva, análise preditiva e análise prescritiva.

Análise descritiva: a grande questão é saber se o facto aconteceu e qual a razão.

Análise preditiva: procura-se responder sobre uma questão para o futuro, o que irá ou poderá acontecer.

---

[41] Segundo publicação de J. Trant (Universidade de Toronto) quando realizou um estudo social sobre o tema *Tagging*. Em *Journal of Digital Information*. TRANT, Jennifer e WYMAN, Bruce - *Investigating social tagging and folksonomy in artmuseums with steve museum*. [Em linha]. [2006]. [Consult. 12 jan. 2019]. Disponível em WWW:<URL:http://www.ra.ethz.ch/cdstore/www2006/www.rawsugar.com/www2006/4.pdf >.

[42] Rank MyApp - *M-commerce*: o que é e qual o diferencial para os negócios? [Em linha]. [2018]. [Consult. 15 jan. 2019]. Disponível em WWW:<URL:https://www.rankmyapp.com/pt-br/mercado/m-commerce-o-que-e-e-qual-o-diferencial-para-os-negocios/ >.

Análise prescritiva: possuindo a resposta da análise descritiva e preditiva o que se almeja é dar a resposta à questão sobre quais as providências que deverão ser tomadas, sobre o que se deverá fazer. Contudo, as consultas dos mesmos dados poderão ter respostas diferentes, dependendo do tipo de pergunta feita (LEAL, 2017).

Por seu turno, Ana Alves Leal (2017) distingue os passos da análise preditiva:

-Identificação ou a finalidade do problema a que a análise pretende responder;

-Delimitação do universo de dados submetidos a análise;

-A identificação de padrões importantes a partir desses dados e

-A associação desses padrões a determinados resultados.

A utilização desses resultados auxilia na tomada de decisões.

Desta forma, na análise preditiva, existe a tarefa de construir e utilizar modelos que façam previsões com base em dados históricos. O conceito de previsão se dá em sentido amplo, com a associação de um valor a uma variável desconhecida. Como exemplo dessa análise temos, a previsão de preços, a avaliação de riscos, o planeamento nos tratamentos de saúde, previsões meteorológicas, entre outras[43].

Sendo a análise preditiva a que tem como finalidade medir probabilidade de resultados futuros, a partir de dados históricos, é a utilizada pelo *Big Data*. É uma análise correspondente ao processo de identificação de padrões. Podendo, ao utilizar essa ferramenta, adaptar-se no presente as tendências futuras, o que para as empresas seria uma ótima opção de investimento, uma vez que as vendas de produtos personalizados aumentam a chance de vendê-los, garantindo assim os seus lucros.

Importa notar que, existem riscos no que toca às tecnologias preditivas, quando as decisões que são tomadas, referente às pessoas, sejam exclusivamente efetuadas pela Inteligência Artificial.

Recorrendo ao uso de *Big Data* as instituições financeiras podem, por exemplo, decidir a respeito da elegibilidade de um cliente específico para a concessão de um crédito, analisar com mais rigor a confiabilidade do mesmo[44]. O resultado de tal análise é obtido

[43] CORDEIRO, António Menezes; OLIVEIRA Ana Perestrelo e DUARTE Diogo Pereira - ***FinTech* – Desafios da Tecnologia Financeira**. Coimbra: Almedina, 2017, p. 82.
[44] LEAL, Ana Alves - *Big data* e proteção de dados pessoais – Desafios à luz do Regulamento Geral de Proteção de Dados. **Revista Vida Judiciária**. Maio/junho 2018.

através de uma técnica chamada de *machine learning*, sem intervenção humana, o que pode resultar em falsas informações.
Com base nessas informações a realização de negócios jurídicos pode ser uma forma de exteriorizar uma grande injustiça, fomentando a discriminação, ou sendo as informações verdadeiras, poderemos ter um outro tipo de problema, que é a criação de perfis completos, principalmente para efeitos comerciais, com todas as preferências, interesses e afinidades de uma pessoa.

1.7 *Lex Data* e o Comércio dos Dados

O mundo em linha mostra-se cheio de oportunidades, uma forma mais barata e mais rápida para se alcançar o desiderato empresarial. A cada dia que passa observa-se que os maiores beneficiados com o uso de *Big Data* são as grandes empresas, mesmo sabendo-se que já existem programas de análise de *Big Data* para as PMEs[45].

Ao aderir um serviço de uma empresa, seja ela de fornecimento de água, telecomunicações ou outras quaisquer, as pessoas fornecem os dados básicos para a concretização do serviço a aderir. Antes da entrada em vigor do Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho de 27 de abril de 2016[46], tais dados eram vendidos de forma ilegal para outras empresas, as quais iniciavam o envio de publicidade, ligações e tudo o mais que fosse possível para que as pessoas contratassem serviços com as respetivas empresas.

Os dados produzidos pelo acesso do utilizador à internet, também eram vendidos para outras empresas, assim como acontecia fora da internet, oferecendo benefícios e vantagens

[45] Com relação às PMEs (pequenas e medias empresas), veja-se às palavras proferidas por Carla Iva Vieira: "Tendo em consideração a lógica de um mercado único, sem fronteiras, as empresas deveriam ser objetos de um tratamento uniforme e baseado num conjunto de regras comuns. Justifica-se, portanto, que a comunidade europeia recomende uma classificação uniformizada a ser aceite pelos Estados – Membros. Nos termos do artigo 48º, 81º e 82º do Tratado que instituiu a Comunidade Europeia e ainda segundo a interpretação que lhes foi dada pelo Tribunal de Justiça das Comunidades Europeias – que "deve considerar-se como empresa qualquer entidade que, independentemente da sua forma jurídica, exerça uma atividade económica, incluindo, designadamente, as entidades que exerçam uma atividade artesanal e outras atividades a titulo individual ou familiar, as sociedades de pessoas ou as associações que exerçam regularmente uma atividade económica." (art.º 1º do Anexo). De acordo com o art.º 2º do Anexo à Recomendação, considera-se: Média empresa – a que emprega menos de 250 pessoas, e tem um volume de negócios que não exceda os 50 milhões de Euros, ou cujo balanço total anual não é superior a 43 milhões de Euros; Pequena empresa: a que emprega menos de 50 pessoas e não ultrapassa os 10 milhões de Euros nos restantes indicadores; Microempresa: a que emprega menos de 10 pessoas e não ultrapassa os 2 milhões de Euros, no que se refere ao volume de negócio ou o seu balanço total anual". VIEIRA, Carla Iva - **Guia Prático de Direito Comercial**. Coimbra: Almedina, 2016, p. 32 e 33.
[46] 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).

patrimoniais com essa transmissão de informação confidencial. O caos estava plantado, porque não se tinha o controlo do que era vendido e muito menos de quem vendeu.

Pode-se falar em uma suposta *Lex Data*, assim como a *lex mercatoria* e a *lex petrolea* eram reguladas pelos comerciantes, e não reguladas por uma autoridade única, evoluindo a partir dos usos e costumes, como se fosse um corpo de regras próprias, criado na vida prática e longe dos Parlamentos.

A comercialização de dados pessoais na maioria das vezes é habitual, ilícita e era ciente por todos e não regulada por nenhuma entidade.

Assim sendo, e perante esta situação hodierna, o Parlamento Europeu veio reforçar que o tratamento de dados pessoais é um direito fundamental, com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (doravante RGPD). Este regulamento tem como objetivo o bom funcionamento do mercado interno, como finalidade o alcance harmonioso do mercado único europeu, pautado em segurança, liberdade, justiça, união económica e progresso.

A presente dissertação vem apresentar como tema "O Uso de *Big Data Analytics* e o Reflexo nos Negócios Jurídicos à Luz do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016", não possuindo a pretensão de tratar exaustivamente os problemas jurídicos suscitados da relação de recolha, armazenamento e tratamento de dados e a realização de contratos.

Houve inúmeras mudanças em vários sectores, a consequência no âmbito jurídico não foi diferente, pelo que a finalidade da presente dissertação é contribuir para o estudo jurídico desta realidade, pretendendo assim, ser norteada por uma tentativa de resposta à seguinte pergunta:

A questão que se apresenta é à luz do Regulamento Geral de Proteção de Dados. Até que ponto se admite a recolha de dados pessoais na internet, e em que momento pode essa informação ser usada na esfera dos negócios jurídicos?

Atualmente, os legisladores, tanto os nacionais quanto os europeus, procuram desenvolver leis que permitam uma concorrência mais justa, transparente, uma maior segurança para os utilizadores em linha, uma maior proteção de dados através de uma adaptação adequada da legislação à realidade atual.

CAPÍTULO II- LEGISLAÇÃO SOBRE PROTEÇÃO DE DADOS

2.1 Os Dados e o Direito

Na União Europeia o direito é formado pelos tratados e pelo direito secundário, sendo os tratados:

- O Tratado da União Europeia – TUE e

- O Tratado sobre o Funcionamento da União Europeia – TFUE.

Todos os Estados-Membros aprovaram os referidos tratados, e são reconhecidos como sendo de direitos primários da União Europeia.

Os de direitos secundários são:

- Os regulamentos;

- As diretivas e

- As decisões da União.

Normas que foram adotadas pelas instituições da União derivadas da competência que lhe foi atribuída pelos tratados (LOPES, 2002).

A Lei das leis, é a expressão imediata dos valores jurídicos acolhidos na comunidade política, é um instrumento precioso de segurança dos cidadãos diante do poder, sendo a soberania do Estado a ponte entre a ordem interna e a ordem internacional[47]. Em relação ao cenário mundial, a Constituição é a representação que enquadra as leis provenientes do Estado. Ao citar Georges Burdeau, Jorge Miranda (1996) faz a afirmação que a Constituição é um início e não um resultado. Em relação à norma já era defendido que as pessoas necessitam sedimentar que ninguém possui outro direito que não seja o de cumprir sempre o seu dever, para que ocorra a regeneração legislativa (COMTE, 1890).

Assim, importa fazer referência - não tão alargada, quanto seria possível ou necessário – ao Art.º 35.º da Constituição da República Portuguesa, que reza a utilização da informática. Onde está definido o direito de acesso aos dados informatizados e o conteúdo que orbita nessa matéria, ainda traz a definição de dados pessoais, como sendo todos os dados que

[47] MIRANDA, Jorge - **Manual de Direito Constitucional Tomo II**. Coimbra: Coimbra Editora, 1996, p. 67.

digam respeito ao cidadão e a proibição de acesso a dados pessoais de terceiros, salvo em casos excecionais (FARIA, 2010).

Também com o mesmo propósito, o Art.º 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, tutela o direito das pessoas, de além de terem o direito a proteção dos dados pessoais, também poderem aceder os dados que lhes digam respeito e a sua retificação. No mesmo sentido, vai o Art.º 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) e a Convenção 108.

A matéria em apreço objetiva tutelar de forma harmoniosa a União, sendo o principal instrumento jurídico sobre proteção de dados. Atualmente o Regulamento Geral de Proteção de Dados que entrou em vigor em 25 de maio de 2018 e substituiu a Diretiva 95/46/CE e a lei interna de proteção de dados, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses.

O RGPD entra num cenário que se integra num pacote legislativo de carácter mais amplo, que versa a matéria de proteção de dados. Assim, almeja-se possíveis transformações na prática jurídica. À luz deste enquadramento, torna-se importante analisar os impactos do *Big Data* na proteção dos dados pessoais e as barreiras que estão a ser levantadas em relação às empresas que beneficiavam de tal tecnologia para auferir lucros.

O RGPD é fruto de um longo processo de aprovação. Possui como característica um texto complexo, onde a compreensão dos 99 artigos depende de leitura dos 173 considerandos. A complexidade do texto é no sentido de possuir conceitos relativamente vagos que direcionam às remissões para o direito interno de cada país. Observa-se artigos longos possuindo muitas alíneas. A título exemplificativo o Art.º 83 do RGPD que depende do legislador português, no que refere aos limites materiais e sancionatórios impostos[48].

2.2 A Nova Definição de Dados Pessoais

Tendo em vista assegurar a compreensão da nova definição de dados pessoais, é importante ressaltar o Art.º 4.º, número 1 do RGPD, que cita serem dados pessoais toda informação relativa a uma pessoa singular identificada ou identificável. Posto isto, a pessoa poderá ser identificável de forma direta ou indiretamente. A forma direta pode-se dizer que é baseada

[48] INA - Características do RGPD. [Em linha]. [2018]. [Consult. 18 jan. 2019]. Disponível em WWW:<URL:https://www.ina.pt/index.php/formacao-noticias/1856-formacao-ina-rgpd>.

no número de identificação civil, no nome, dados de localização, identificadores por via eletrónica; A forma indireta que é através de elementos específicos de identidade física, fisiológica, genética, cultural entre outras. Nota-se um alargamento na definição do conceito de dados pessoais, o que deixa as empresas em alerta nessa questão, bastando conseguir identificar a pessoa, no meio dos demais utilizadores, para que se esteja a tratar de dados pessoais.

Em conformidade com o novo conceito de dados pessoais, pode-se fazer uma análise prática, quando se pensa em *cookies* (que são minis arquivos de texto que se mantêm ativo nos computadores, e interagem identificando os utilizadores e memorizando o comportamento enquanto estiverem conectados à internet, sendo atribuído um código para a identificação de cada pessoa conectada)[49], *downloads*, *passwords*, *IPs*, *URL* entre outros, que todas essas informações levam diretamente ao utilizador certo e determinado em linha, sendo desta forma dados pessoais. Assim, toda empresa que utilizar a ferramenta *Big Data*, nestes casos há grande possibilidade de estar a manusear dados pessoais conforme o RGPD.

Quanto à relação entre *Big Data* e a identificabilidade das pessoas, observa-se que quase todos os atos realizáveis nos dispositivos e computadores ligados à internet, são rapidamente detetados sendo na sua grande maioria dados pessoais.

Importa trazer a diferença do conceito de dados pessoais atual do anterior ao RGPD. No conceito anterior ao Regulamento era preciso uma identidade civil para ser considerado como dados pessoais. Atualmente não necessita de existir um número de identidade civil, basta um código de identificação ou algo similar, que consiga separar o utilizador dos demais utilizadores para serem considerados dados pessoais.

Alguma polémica sobre o assunto assume o cenário dos aplicadores do direito, onde se defende que existe uma grande rigidez e amplitude do conceito oriundo do Regulamento[50]. Independentemente da fonte de recolha do *Big Data* os dados podem ser pessoais ou não, o que resulta na aplicação do RGPD somente no primeiro caso.

A criação de conteúdo oriunda de vários suportes como áudio, vídeo, texto e imagem, que podem ser relativos às pessoas singulares ou pessoas coletivas, como exemplo dados de

[49] *European Commission – Cookies*. [Em linha]. [2018]. [Consult. 25 nov. 2018]. Disponível em WWW:<URL:http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm>.
[50] Grupo de Trabalho do Artigo 29.º - Parecer 4/2007 sobre o conceito de dados pessoais (UE) 2016/679 (01248/07/PT WP136). p6. [Em linha]. [2007]. [Consult. 2 jan. 2019]. Disponível em WWW:<URL:https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>.

tráfegos, imagens de satélites, imagens meteorológicas, dados de mercado de intercâmbios financeiros em todo o mundo e não pode ser atribuído o conceito "amplo" constante no RGPD, por serem dados operacionais e não poderem ser relacionados a nenhuma pessoa singular[51]. Portanto, a definição ora constante no RGPD não é rígida ou ampla de mais, apenas ampara o direito das pessoas de serem tutelados no que tange aos dados que lhes dizem respeito, tratando-se de preferências e tendências avaliáveis de forma automatizada.

Como é sabido por todos, não existe uma forma de blindagem infalível, e medidas técnicas e organizacionais apropriadas estão longe de serem perfeitas. Como resultado, as obrigações regulatórias para notificações de violação de dados, recuperação de desastres de dados, transparência, entre outros, devem fazer parte dos contratos de Tecnologia de Informação e Comunicação e os cidadãos.

2.3 Princípios à Luz do Regulamento Geral de Proteção de Dados

Observa-se que a palavra princípio – *principium*- que pela definição da palavra é o início, ou seja, o ponto de partida, deve também significar seguir as regras, ou seja as normas (PORTANOVA, 1999, p.13). Desta forma, deve-se sempre basear qualquer tratamento de dados pessoais analisando se respeita todos os princípios elencados no RGPD[52] [53].

Com o amadurecimento das normas, os princípios ganharam força normativa, sendo que um dos primeiros doutrinadores a afirmar tal caráter normativo foi Crisafulli (BONAVIDES, 2006, p. 257).
Os princípios como poder vinculativo têm a força normativa de tornar inválidas todas as decisões e quaisquer atos que vão de encontro aos mesmos[54].

Atualmente os princípios que norteiam a matéria de proteção de dados pessoais são:

---

[51] SUPRIYADI, Daniar - *Personal and Non-Personal Data in the Context of Big Data*. [Em linha]. [2017]. [Consult. 19 jan. 2019]. Disponível em WWW:<URL:http://arno.uvt.nl/show.cgi?fid=142300>.
[52] A definição de princípios pode ser entendida como: "A doutrina utiliza o termo 'princípio' com muitas significações: critério, política, sistema, requisito e regra, por exemplo",). PORTANOVA, Rui - **Princípios do processo civil**. Porto Alegre: Livraria do Advogado, 1999.
[53]LUCON, Paulo Henrique dos Santos - Garantia do tratamento partidário das partes. Garantias constitucionais do processo civil. **Revista dos Tribunais**. Vol 1. n. º 1 (1999). São Paulo: Revista dos Tribunais, p.92.
[54] ESPÍNDOLA, Ruy Samuel - **Conceito de Princípios Constitucionais**. 2. ed. rev. ampl. e atual. São Paulo: Revista dos Tribunais, 2002, p. 60.

- Licitude, Lealdade e Transparência[55];

- Limitação das Finalidades[56];

- Minimização dos Dados[57];

- Exatidão[58];

-Limitação da Conservação[59];

- Integridade e Confidencialidade[60] e

- Responsabilidade[61].

Sendo assim merece atenção, embora limitada, de uma explanação sobre cada um dos princípios. A importância dos mesmos se faz presente na dissertação por ser a base da tutela dos dados pessoais em que a sociedade da informação vive atualmente, e no mundo *Big Data* é de importância sumária o conhecimento dos meios que se pode dispor para evitar possíveis danos.

2.3.1 Princípio da Licitude, Lealdade e Transparência

O princípio da licitude defende a forma como devem ser tratados os dados pessoais. Com íntima ligação com o Art.º 6.º e 9.º do RGPD. O referido princípio tem como objetivo fazer cumprir as normas de direito interno e da União, tendo como alicerce os princípios gerais do direito.

O mesmo princípio rege a forma como os dados devem ser disponibilizados pelos titulares, para que seja um tratamento lícito. Pode ser aplicado de duas maneiras, através:

- Do Consentimento[62] ou

[55] Art.º 5.º, a) do RGPD.
[56] Art.º 5.º, b) do RGPD.
[57] Art.º 5.º, c) do RGPD.
[58] Art.º 5.º, d) do RGPD.
[59] Art.º 5.º, e) do RGPD.
[60] Art.º 5.º, f) do RGPD.
[61] Art.º 5.º, n. º2 do RGPD.
[62] O Consentimento está previsto no Art.º 6.º, n. º1, alínea a) do RGPD, as demais alíneas do mesmo artigo amparam outros fundamentos para a realização do tratamento. Será considerado válido o Consentimento que seja o externar de uma vontade baseada por um ato de manifestação livre, específica, informada e explícita. O ato deverá ser de declaração ou ato positivo, conforme artigo 4.º n.º 11 do RGPD.

-Fundamento legítimo previsto por lei.

Assim, somente destas formas o tratamento de dados pessoais é considerado lícito, sendo o Responsável pelo Tratamento[63] (doravante RT) a pessoa quem deverá fazer cumprir as obrigações legais as quais esteja sujeito[64].

O princípio da lealdade é regido pelo senso de confiança que deve ser estabelecido entre o RT e as pessoas titulares dos dados pessoais a serem tratados, é um princípio colaborador de uma relação baseada na transparência e segurança jurídica. Possuindo como característica a tentativa de uma relação de equilíbrio entre o RT, subcontratantes e os titulares dos dados pessoais[65].

E por último o princípio da transparência, que tem como característica a publicidade do tratamento, com maior controlo pelos titulares dos dados, como exemplo a plataforma do Facebook que permite que os utilizadores tenham acesso ao "Registo de Atividades", remetendo para todas as atividades que foram realizadas pelos titulares. Isto não significa que se esgote todo o tipo de tratamento que é realizado, é somente as atividades dos titulares da conta. O princípio da transparência deve abranger também as atividades do RT.

Logo, o princípio da transparência deverá favorecer o conhecimento pelos titulares dos dados pessoais se os mesmos estão a ser tratados ou se virão a ser tratados, o que deverá ser de fácil acesso e compreensão com linguagem clara e simples. Também deverá ser exposto de forma clara a identidade do RT, assim como os fins do tratamento. Desta forma, objetiva-se que seja salvaguardado o direito de obter a confirmação e comunicação dos dados pessoais que estão a ser tratados. A comunicação nos casos de riscos deverá ser alertada aos titulares, assim como as regras, garantias e direitos associados ao tratamento dos dados pessoais[66].

[63] No artigo 4.º, n.º 7 do RGPD está a definição do responsável pelo tratamento, como sendo a pessoa ou o organismo que determina as finalidades e os meios de tratamento. Assim dispõe: "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".
[64] Considerando 40 do RGPD.
[65] PINHEIRO, Alexandre Sousa [et al.] – **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina. 2018, p. 205.
[66] Considerando 39 do RGPD.

2.3.2 Princípio da Limitação das Finalidades

Os dados recolhidos devem ter finalidades determinadas, explícitas e legítimas sendo proibido o uso dos dados para outras finalidades. Não são consideradas outras finalidades, de acordo com o Art.º 89.º, n. º1 do RGPD, quando os dados sejam utilizados para:

- Fins de arquivo de interesse público;

-Fins de investigação científica;

- Fins históricos e

- Fins estatísticos.

Deverão ser evitadas ambiguidades, frases genéricas e a utilização de idiomas estrangeiros. As finalidades devem estar expostas de forma clara, explícita e determinada, para que se evitem equívocos.

O princípio da limitação das finalidades é considerado relevante, sendo um passo importante no que tange o tratamento de dados pessoais, com imposição crucial e primeira justificação para a realização de tratamento de dados[67].

2.3.3 Princípio da Minimização dos Dados

Os dados devem ser adequados, pertinentes e limitados somente ao que é necessário às finalidades que foram recolhidos. Como finalidade específica de limitar a conservação dos dados por período necessário, cabe ao RT fixar o prazo para o apagamento dos mesmos. Há uma delimitação entre a necessidade imposta pelas finalidades.

2.3.4 Princípio da Exatidão

Os dados pessoais devem ser corretos e atualizados sempre que for necessário. Os dados inexatos devem ser apagados ou retificados, sempre observando as finalidades da recolha.

[67] PINHEIRO Alexandre Sousa - ***Privacy*** **e proteção de dados pessoais: a construção do direito à identidade informacional.** Lisboa: AAFDL, 2015, p. 826.

2.3.5 Princípio da Limitação da Conservação

Os dados pessoais devem poder identificar os titulares, porém, deve ser somente durante o período necessário para atender as finalidades que justificam o tratamento.

Os dados pessoais como regra devem ser mantidos por um espaço de tempo igual as finalidades propostas, porém, admite-se a conservação por um período mais longo nos casos de serem tratados exclusivamente para:

- Fins de arquivo de interesse público;

- Fins de investigação científica;

- Fins de investigação histórica ou

- Fins estatísticos.

Tendo como finalidade salvaguardar os direitos e as liberdades dos titulares dos dados.

2.3.6 Princípio da Integridade e Confidencialidade

O tratamento dos dados deve ser feito a garantir a sua segurança, neste sentido entende-se:

- Proteção ao tratamento não autorizado;

- Proteção ao tratamento ilícito;

- Proteção contra a perda;

- Proteção contra a destruição;

- Proteção contra a danificação acidental.

Assim, deverão ser adotadas medidas adequadas, de forma técnica ou organizativa, para resguardar este princípio.

2.3.7 Princípio da Responsabilidade

O RT é o detentor deste princípio, pois, fica da sua inteira responsabilidade fazer cumprir o Art.º 5.º, n.º 1 do RGPD (licitude, lealdade e transparência).

Por isso tudo, observa-se que os princípios precedentes podem ser classificados como a "Constituição" do RGPD, pois, apresentam origem na Convenção 108 em seu Art.º 5.º e no Art.º 6.º da Diretiva 95/46/CE[68].

2.4 Anonimização e Pseudonimização

Os princípios norteadores de proteção de dados devem ser aplicados para as informações pessoais de qualquer pessoa, sendo identificada ou identificável[69].

O pseudónimo é um meio de proteção de dados pessoais que tem como finalidade dificultar a identificação de pessoas. Os dados pessoais que tenham sido pseudonimizados possuem a capacidade de identificar um utilizador dos demais. Nos casos em que recorrem ao aparelhamento com outras informações, são considerados dados identificáveis, ou seja, podem ser geridos pelo RT. Dado o exposto, é de aplicação imediata o RGPD.

A pseudonimização é uma forma de desidentificação que não sendo emparelhada com informações suplementares, não pode identificar o utilizador[70].

A utilização de pseudónimos não é um método de anonimização de dados pessoais, apenas cria maior dificuldade no que toca a possibilidade de correspondência de um conjunto de dados à identidade original do titular dos dados, sendo desta maneira uma medida de segurança[71].

Também é de suma importância citar a encriptação[72], tecnologia importante no ciberespaço que é o meio utilizado para criar pseudónimos, através de uma chave criptográfica apenas

---

[68] PINHEIRO, Alexandre Sousa [et al.] – **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina. 2018, p. 205.
[69] Segundo o Considerando 26 do RGPD.
[70] CORDEIRO, António Menezes; OLIVEIRA Ana Perestrelo e DUARTE Diogo Pereira - ***FinTech* – Desafios da Tecnologia Financeira**. Coimbra: Almedina, 2017, p. 112.
[71] Grupo de Trabalho do Artigo 29.º - Parecer 05/2014 sobre técnicas de anonimização (UE) (0829/14/PT GT216). [Em linha]. [2014]. [Consult. 20 jan. 2019]. Disponível em WWW:<URL:https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831045040634.pdf >.
[72] Dicionário Priberam – Definição de Encriptação. [Em linha]. [2017]. [Consult. 05 dez. 2018]. Disponível em WWW:<URL:https://dicionario.priberam.org/encripta%C3%A7%C3%A3>.

conhecida pelo RT de dados, para que possa ter acesso às informações em momento adequado.

A matéria em apreço está regulada no Art.º 4.º, nº5 do RGPD, ao definir o que venha a ser a pseudonimização, que são os dados que deixam de poder ser atribuídos a um titular sem recorrer a informações suplementares.

Na anonimização dos dados, estes não podem estar associados a uma pessoa. Como o seu titular não pode ser identificado, se tomadas as providências cabíveis que garantam a eficácia do uso da técnica, não cabe a aplicação do RGPD.

De acordo com o Considerando 26, para anonimizar quaisquer dados, têm de lhes ser retirados elementos suficientes para que deixe de ser possível identificar os titulares. Com a aceleração tecnológica, fica o Responsável pelo Tratamento de dados com o encargo de rotineiramente reavaliar os riscos inerentes deste meio.

Segundo o Grupo de Trabalho do Artigo 29/ 0829/14/PT, ao realizar uma análise jurídica do tema anonimização, obteve quatro características principais:

- Que a anonimização pode ser um extrato do tratamento de dados pessoais;

- Que tem como foco a irreversibilidade referente à identificação do titular;

- Que há a possibilidade de várias técnicas de anonimização, não existindo qualquer norma que verse sobre o assunto na legislação europeia e

- Que deverá ser observado o avançar tecnológico no conjunto dos meios possíveis de identificação e avaliação dos riscos pelo RT e terceiros.

Uma forma exemplificativa da realidade fáctica, de como a anonimização possui ainda riscos no que tange a identificação dos usuários, pode-se destacar que 87% dos norte-americanos podem ser identificados quando ocorre o cruzamento de dados que tenham sido anonimizados, como por exemplo código postal, género e a data de nascimento[73].

Como resultado, o risco presente na questão da anonimização e na não-aplicação do RGPD, levanta um certo sentimento de desamparo legal. Os algoritmos evoluem com uma velocidade muito grande e não era de se estranhar que mais cedo ou mais tarde a

[73] SWEENEY, Latanya - *Simple Demographics Often Identify People Uniquely*. [Em linha]. [2000]. [Consult. 27 set. 2018]. Disponível em WWW:<URL:https://dataprivacylab.org/projects/identifiability/paper1.pdf >.

combinação entre dados anonimizados (fraca anonimização) pudesse quebrar a barreira do desconhecido.

Em virtude do que foi mencionado, *a priori* não é aplicável o RGPD quando exista a anonimização de dados, por força do Considerando 26, porém com a condição de não-reconhecimento de uma pessoa singular. Isto significa que, sendo possível a identificação direta ou indireta de uma pessoa, mesmo que os dados tenham sido anonimizados cabe sim a aplicação do RGPD. O legislador, já prevendo uma evolução tecnológica rápida, deixou claro que: "tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica". *C*onforme o dispositivo legal, as medidas poderão variar.

2.5 Dados Sensíveis

O RGPD traz como definição de dados sensíveis[74] ou dados de categoria especial, como sendo os dados que merecem proteção específica. São os dados que apresentam sensibilidade[75] na esfera dos direitos e liberdades fundamentais. São os dados que possam revelar:

- Origem racial;

- Origem étnica;

- Opiniões políticas;

- Convicções religiosas;

- Convicções filosóficas;

- Filiação sindical;

- Tratamento de dados genéticos;

- Dados biométricos;

- Dados relativos à saúde;

- Dados relativos à vida sexual e

[74] Considerando 51 do RGPD.
[75] Art.º 9.º do RGPD.

- Orientação sexual.

É proibido o tratamento destes dados como regra. Porém, o mesmo é lícito nos casos em que:

- O titular dos dados tiver dado o Consentimento, que seja explícito para o tratamento desses dados;

- Se for necessário para o cumprimento de obrigações e para o exercício de direitos específicos do RT;

- Se o tratamento for para proteger interesses vitais seja do titular dos dados ou de pessoa singular;

- Se o tratamento for no âmbito das suas atividades legítimas, resguardado as garantias adequadas por quaisquer organismos sem fins lucrativos. O tratamento deverá se referir aos membros do grupo, ou antigos membros, e não poderá ser fornecido a terceiros sem o Consentimento dos titulares;

- Se os dados pessoais tiverem sido tornados público pelo titular;

- Quando da necessidade da declaração num processo judicial, tendo como finalidade a defesa de um direito ou o exercício do mesmo;

- Sempre que os tribunais exercem a sua função jurisdicional;

- Quando o tratamento for necessário para interesse público, salvaguardando os direitos fundamentais, baseado no direito da União ou de um Estado-membro;

- Quando o tratamento for necessário para medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social, sempre com base no direito da União ou dos Estados-Membros ou nos casos de um contrato com profissional de saúde;

- Quando for de interesse público na esfera da saúde pública, nos casos de ameaças transfronteiriças ou para assegurar um elevado nível de qualidade e segurança da saúde, medicamentos e dispositivos médicos e

- Para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos.

Em todas as situações deverá sempre levar em consideração o direito da União ou dos Estados-Membros, assim como os direitos e liberdades dos titulares dos dados.

Um exemplo sobre dados que revelam origem racial: o Estado português tem como finalidade usar o Censo de 2021 para recolher dados sobre discriminação e desigualdade em Portugal. A questão foi debatida, em 05-02-2018, pelo grupo de trabalho formado pela Secretaria de Estado para a Cidadania e Igualdade. O extrato desses dados, permitirá saber qual a composição étnico-racial da população portuguesa. São dados sensíveis a serem tratados, e são dados em larga escala, que podem ser comparados com dados de outros países e mesmo internamente, pelo que deverão ser usados todos os meios adequados para que não ocorra o perigo de quebra de sigilo. A tecnologia *Big Data* também se alimenta de dados como os supramencionados. Por serem dados pessoais e por revelarem origem racial deverá ser aplicado o RGPD.

Outro exemplo, agora sobre dados relativos à saúde: através da Plataforma de Dados da Saúde (PDS)[76] criada em junho de 2012, é possível que as pessoas (utentes) e os profissionais da saúde tenham acesso às informações, mesmo os profissionais que estejam fora do Serviço Nacional de Saúde (hospitais privados).

A Plataforma de Dados da Saúde permite que mais de 370 instituições tenham acesso a dados clínicos de pacientes. Os dados são armazenados em cinco bases de dados centrais, cobrindo todos os cuidados de saúde primários, todos os hospitais públicos e privados. Mais um exemplo de *Big Data* e dados sensíveis, em que a administração desses dados deverá resultar numa organização muito detalhada e organizada entre os responsáveis pelo tratamento e os titulares dos dados.

A quebra de sigilo desses dados pode resultar em graves danos para os titulares, e em alguns casos em fator discriminatório no momento da realização contratual e consequentemente reflexo na esfera jurídica do mesmo. Por esta razão e por outras, os dados de saúde são considerados dados sensíveis, e somente poderão ser objeto de tratamento para fins relacionados com a saúde[77]. De outra forma deverá ser observado o direito da União ou dos Estados-Membros, ficando estabelecido que os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições em relação ao tratamento desses dados.

[76] Serviço Nacional de Saúde – PDS – Plataforma de Dados da Saúde. [Em linha]. [2018]. [Consult. 27 out. 2018]. Disponível em WWW:<URL:https://spms.min-saude.pt/2013/11/pds-plataforma-de-dados-da-saude/>.
[77] Considerando 53 do RGPD.

Uma pergunta que se pode fazer é a de saber quem é o responsável pelo tratamento dos dados, principalmente nos casos de esclarecimentos, correções de dados, atualizações, quebra de sigilos de dados pessoais, etc., uma vez que os dados pessoais e sensíveis, são utilizados por vários hospitais e consequentemente todos os médicos. Observa-se uma situação confusa e comprometendo a proteção dos seus direitos. A autoridade pública que for responsável por tal partilha, deve ser considerada corresponsável pelo tratamento dos dados pessoais dos utentes e o ponto de contato para esclarecimento dos mesmos[78].

Pelo exposto, todas as situações em que os dados pessoais tiverem natureza de dados sensíveis, dever-se-á recorrer à aplicação do Art.º 9.º do RGPD, sempre com atenção redobrada no que toca o Consentimento e a sua transparência ou se os dados tiverem sido tornados público pelo titular dos mesmos.

[78] GT29.º Sobre a Proteção de Dados - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante». (UE) 00264/10/PTWP169 16 de fevereiro de 2010, p. 29. [Em linha]. [2018]. [Consult. 27 out. 2018]. Disponível em WWW:<URL:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_pt.pdf>.

CAPÍTULO III – O NOVO MODELO ADOTADO PELO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

3.1 Abordagem Baseada no Risco e a Abordagem de Autodefesa

Nos termos do Art.º 288.º do Tratado de Funcionamento da União Europeia (TFUE), todo o regulamento tem carácter geral, sendo obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros. Desta maneira, o RGPD é de aplicação imediata para todos os países da União Europeia.

Grande parte da matéria sobre dados pessoais elencada na Diretiva 95/46/CE, que foi revogada, se manteve, como por exemplo os objetivos e princípios. Porém, houve algumas novidades, sendo de suma importância ressaltar algumas transformações na referida matéria, que foi ajustado à rápida evolução tecnológica, como as novas formas de partilha, tratamento e transmissão de dados.

A legislação valeu-se de precauções a serem tomadas, para que a economia digital do mercado interno seja coroada pela confiança necessária ao seu bom desenvolvimento[79], amparada por uma maior confiança jurídica.

O RGPD não traz nenhum regime jurídico direcionado exclusivamente para o tratamento de dados via *Big Data*[80]. Porém, inova num modelo de regulação aplicável para todos os tipos de dados. Esse novo modelo é baseado numa Abordagem Baseada no Risco e numa Abordagem de Autodefesa.

A regulação de *Big Data* está incluída na tutela geral da proteção de dados. Porém, pode-se identificar alguns artigos voltados à sua regulamentação, que seguem na dissertação.

[79] Considerando 6 e 7 do RGPD.
[80] LEAL, Ana Alves - *Big data* e Proteção de Dados Pessoais – desafios à luz do Regulamento Geral de Proteção de Dados. **Revista Vida Judiciária**. Maio/junho 2018, p.19. Disponível em WWW:<URL: http://www.cidp.pt/Archive/Docs/f826818695653.pdf >.

3.2 Abordagem Baseada no Risco

De acordo com o Art.º 35º e 36º do RGPD, institui dois procedimentos a serem adotados. O primeiro é um procedimento realizado previamente através de uma Avaliação de Impacto sobre a Proteção de Dados e a Consulta Prévia.

3.3 Avaliação de Impacto sobre a Proteção de Dados (AIPD)

O procedimento comumente, em inglês, chamado de «*DPIA*» (*Data protection Impact Assessment*)[81], é a avaliação de impacto sobre a proteção de dados (doravante AIPD) quando implicar um elevado risco para os direitos e liberdades das pessoas singulares, devendo ser realizada de forma prévia pelo RT, ou seja, antes do tratamento dos dados. Tem como características principais a observação das situações em que são utilizadas as novas tecnologias, levando em consideração a natureza, âmbito, contexto e finalidades.

É um processo que possui duas finalidades:

- Estabelecer e cumprir a norma em questão e

- Demostrar inequivocamente que foram usados meios adequados e que os RTs tomaram as devidas precauções, visando assegurar que estão em conformidade com o RGPD[82].

A AIPD é então baseada na chamada avaliação do impacto na privacidade[83], visando o respeito pelos direitos individuais.

A avaliação de impacto representa um papel importante no que toca a questão da responsabilização do RT, proporcionando um meio de prova substancial que demostra a intenção do mesmo.

O RT poderá ser auxiliado por outras pessoas, como:

- O encarregado da proteção de dados, quando este seja designado[84] e

---

[81] Artigo 35 do RGPD.
[82] Grupo de Trabalho do Artigo 29.º - 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. (UE) (17/PTWP 248 rev.01). [Em linha]. [2017]. [Consult. 21 jan. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf >.
[83] O direito à privacidade foi defendido pela primeira vez por Warren e Brandeis numa publicação na HLR, intitulado "*The righ to privacy*". CASTRO, Catarina Sarmento e - **Direito da Informática, Privacidade e Dados Pessoais**. 1ª ed, Coimbra: Almedina, 2005, p. 17.
[84] Art.º 35.º, n. º 2 do RGPD.

- Os titulares dos dados[85].

Para a análise satisfatória da avaliação do risco, deverão ser observados minuciosamente os códigos de conduta que foram aprovados[86].

Torna-se imperioso dominar o conceito do risco em questão, que é conveniente ser de acordo com as definições do GT 29.º, que define como sendo um risco residual[87], ou seja, aquele que ainda exista e permaneça vivo por um lapso temporal razoável. A gestão[88] desse risco também merece atenção especial, pois são atividades coordenadas que visam uma direção e controlo a uma organização referente ao risco.

Sempre que forem utilizadas novas tecnologias, analisada a natureza, o âmbito, o contexto, a finalidade que se pretende alcançar, e colocado em risco elevado o direito sedimentado, como direitos e liberdades das pessoas, deverá ser realizado uma avaliação de impacto. Posto isto, é importante salientar que tal procedimento tem um aspeto temporal que antecede o início do tratamento, sendo sempre realizado antes. Será uma questão de análise realizada pelo responsável pelo tratamento. Num primeiro momento, é de ordem discricionária a realização da AIPD, sendo certo que, em algumas situações a aplicação é obrigatória, como nos casos de tratamento automatizado, tratamento em grande escala – *Big Data*, categorias especiais de dados, condenações penais e infrações e controlo sistemático[89].

Assim sendo, quando se tratar de dados baseados por tratamento automatizado, principalmente quando exista definições de perfis, que geralmente produzem efeitos jurídicos, fica obrigado a realização prévia de AIPD. Como exemplo, uma empresa de seguros que seleciona por perfis de pessoas em redes sociais antes da realização de contrato, fazendo uma análise de quem possa vir a ser um risco para o descumprimento do mesmo. Desta forma, o valor a ser acordado pode ser maior para uns do que para outros, ou mesmo nem sequer manifestar o interesse de concretização de nenhum tipo de contrato com determinada pessoa, verifica-se assim a concretização de uma prática discriminatória.

---

[85] Art.º 35.º, n. º 9 do RGPD.
[86] Art.º 40.º do RGPD.
[87] Grupo de Trabalho do Artigo 29.º - 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 (17/PTWP 248 rev.01), p.18 [Em linha]. [2017]. [Consult. 21 jan. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf >.
[88] *Idem*, p. 7.
[89] Art.º 35, n. º 3 do RGPD.

Não há exemplo melhor do que o supramencionado, uma vez que os critérios avaliativos seriam originários de *Big Data*. Fica claro que os critérios oriundos de tal tecnologia podem ser a avaliação, a construção de perfis, previsões de preferências, decisões automatizadas, tratamento de dados sensíveis, dados processados em larga escala, base de dados que tenham sido relacionadas ou combinadas com outras aplicações inovadoras de base tecnológica entre outros[90].

O GT29 alega ser meramente exemplificativa[91] a lista constante do Art.º 35.º, n.º 4, quando se fala em tratamento automatizado e novas tecnologias, e a amplitude que se pode alcançar. Nos casos em que houver dúvidas sobre a realização da avaliação de impacto, esta deverá ser realizada.

Devido à inexistência de uma lista elencada no RGPD, que procura uma adequação para todos os países da União Europeia para os tratamentos de dados que ficam sujeitos à avaliação de impacto, fica como responsável a Autoridade de Controlo pela elaboração e a publicação de uma lista[92], e outra lista para os dados não sujeitos[93] à avaliação de impacto. As listas têm como finalidade uma abordagem harmonizada no que toca o tratamento transfronteiriço dos dados.

A avaliação de impacto sobre a proteção de dados e a elaboração das referidas listas, resultou num projeto onde todos os países elaboram as suas respetivas listas e submete-as para análise, com a finalidade de estabelecer somente uma, mais harmoniosa e não taxativa, uma vez que há a necessidade de observar a legislação interna de cada país.

O objetivo do RGPD não é chegar a uma lista única dentro da União Europeia, mas aproximar ao máximo possível as similaridades dos factos, para que consiga uma ampla tutela dos direitos das pessoas de forma coerente[94], sendo uma proteção equivalente dos dados para todas as pessoas da União Europeia. Pode-se dizer que a avaliação de impacto é um meio para alcançar a finalidade maior, que é assegurar e comprovar a aplicação correta da legislação, sendo o RT o mentor das ferramentas a utilizar para os devidos fins.

[90] *Idem*, pp. 7 a 9.
[91] *Idem*, p.7.
[92] Art.º 35.º, n. º4 do RGPD.
[93] Art.º 35.º, n. º 5 do RGPD.
[94] O entendimento da coerência feito pela Comissão, revela que é de suma importância a análise feita pelo Grupo de Trabalho 29 que resultou na orientação WP248, sendo uma análise essencial para garantir a coerência da matéria em toda União.

A Comissão Nacional de Proteção de Dados[95] (doravante CNPD), submeteu para análise o seu projeto de lista ao Conselho Europeu para a Proteção de Dados (doravante Conselho), sendo decidido pelo mesmo, que nenhuma lista poderá ser exaustiva.

Dado o exposto, O RGPD não apresenta uma definição de avaliação de impacto, porém, define o conteúdo mínimo[96], não sendo o RT compelido a realizar a avaliação de impacto em todos os casos, somente quando apresentar um elevado risco para os direitos e liberdades das pessoas.

A CNPD em 16-10-2018 apresentou e aprovou a seguinte lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados[97], que se deve acrescentar aos previstos no n.º 4 do Art.º 35.º do RGPD:

"1- Tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde;

2- Interconexão de dados pessoais ou tratamento que relacione dados pessoais previstos no n.º 1 do Art.º 9.º ou no Art.º 10.º do RGPD ou dados de natureza altamente pessoal;

3- Tratamento de dados pessoais previstos no n.º 1 do Art.º 9.º ou no Art.º 10.º do RGPD ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação nos termos da alínea b) do n.º 5 do Art.º 14.º do RGPD;

4- Tratamento de dados pessoais que implique ou consista na criação de perfis em grande escala;

5- Tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos;

6- Tratamento dos dados previstos no n.º 1 do Art.º 9.º ou no Art.º 10.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público,

[95] A Comissão Nacional de Proteção de Dados (CNPD) é a entidade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais.
[96] Art.º 35.º, n. º 7 do RGPD.
[97] CNPD - Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. [Em linha]. [2018]. [Consult. 03 abr. 2019]. Disponível em WWW:<URL:https://fiscalidade.pt/wp-content/uploads/2018/12/regulamento_1_2018.pdf >.

investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares;

7- Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;

8- Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados.

9- Tratamento de dados pessoais previstos no n.º 1 do Art.º 9.º ou no Art.º 10.º do RGPD ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias já existentes."

Por todos esses aspetos, a AIPD possui como finalidade atenuar os riscos e assegurar a proteção dos dados pessoais das pessoas e fazer prova de que houve a preocupação na observância do RGPD[98].

3.4 Consulta Prévia a Autoridade de Controlo

Nos casos em que o tratamento dos dados apresente risco elevado, depois de ter sido realizado AIPD, deverá o RT realizar a Consulta à Autoridade de Controlo, nos termos do Art.º 36.º do RGPD com a finalidade de atenuar os riscos que foram detetados pela AIPD. A referida consulta deverá ser realizada antes de proceder ao tratamento.

No ato da Consulta a Autoridade de Controlo deverá o RT informar[99]:

- A existência de repartição de responsabilidades;

- As finalidades e os meios que foram previstas para o tratamento;

-As medidas e garantias previstas;

- Os contactos do EPD, se houver;

- A AIPD e o seu resultado e

[98] Considerando 90 do RGPD.
[99] Art.º 36, n-º 3 do RGPD.

- Todas as demais informações que a Autoridade de Controlo venha a solicitar.

Então, a Consulta prévia é um procedimento a ser realizado após a AIPD, nos casos em que o risco residual seja detetado[100]. A Autoridade de Controlo, desta forma, analisa o pedido do RT nos casos de afronta ao RGPD[101].

3.4.1 Riscos Inerentes da Tecnologia *Big Data*

A finalidade do RGPD é oferecer às pessoas a possibilidade de possuírem o conhecimento e o controlo dos seus dados pessoais, e o ato que ajuda ao desiderato é o Consentimento para a utilização dos mesmos. A violação dos direitos *online* deverá ser uma preocupação constante do RT.

Numa primeira análise em relação aos dados proveniente de *Big Data*, existem riscos que são inerentes ao tipo de dados a serem tratados e também ao tipo de tratamento de dados. Independentemente de serem tomadas as precauções adequadas, terá que haver sempre a precaução com os riscos residuais[102], ou seja, os riscos perenes, que se possam refletir de forma negativa nos titulares dos dados.

Assim, em relação à tecnologia *Big Data*, o RT tem maior dificuldade em desenvolver análise desse tipo de dados, porque normalmente são dados pessoais e devem ser submetidos ao RGPD. Desta forma, a AIPD e a Consulta prévia à autoridade competente deverão ser sempre realizadas.

Numa segunda análise à mesma tecnologia, ao verificar o Art.º 36.º do RGPD, não fica claro quais são as responsabilidades a serem desempenhadas pela autoridade reguladora, uma vez que os dados resultantes de *Big Data* serão com muita frequência submetidos a esta.

Caso os referidos dados não apresentem um risco de violação do RGPD, mas apresentem perigo iminente de risco, a autoridade competente poderá tomar alguma decisão de forma

---

[100] Grupo de Trabalho do Artigo 29.º - 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 (17/PTWP 248 rev.01), p.18 [Em linha]. [2017]. [Consult. 21 jan. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf>.

[101] Art.º 57.º, n.º 1 e artigo 58.º, n.º 3 do RGPD.

[102] QUELLE, Claudia - *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing*, p.2 [Em linha]. [2017]. [Consult. 6 out. 2018]. Disponível em WWW:<URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2695398>.

negativa para o tratamento destes dados?[103] Este questionamento não possui resposta no RGPD, o que resulta numa possível proposta de reforma.

A solução, frente às incertezas, será de que aos dados provenientes de *Big Data*, quando possam oferecer possíveis riscos, sejam realizados procedimentos e negociações *ad hoc*[104], entre a autoridade competente e o RT.

Quanto aos riscos que norteiam a matéria em questão, é importante esclarecer a forma da lógica como o *Big Data* é constituído.

A lógica é dividida em duas correntes principais que são a indutiva e dedutiva[105], sendo a primeira a mais importante na matéria *Big Data*, estando relacionada com a questão da probabilidade[106]. Sumariamente, importa esclarecer o funcionamento de tais lógicas.

A função da lógica é fazer análise do elo em agentes, entre as premissas e as conclusões. Geralmente quando as premissas são verdadeiras, as conclusões também o serão, o elo entre ambas é categorizado como forte (argumentos dedutivamente válidos, verdadeiros). Noutros casos, quando as premissas são apenas um apoio para se retirar as conclusões, estas não podem ser categorizadas como confiáveis, sendo o elo categorizado como não tão forte (argumentos indutivamente fortes). Sendo assim, os argumentos podem possuir várias intensidades de força[107]. A lógica indutiva utiliza a probabilidade para chegar a uma conclusão. Assim existe uma probabilidade de a conclusão ser verdadeira.

Convém, antes de tudo o mais, explanar a diferenciação em relação o *Big Data* das demais formas tradicionais de análise de dados e do pensamento científico tradicional.

As formas tradicionais de análise de dados, trabalham com a espécie de lógica dedutiva e o pensamento científico tradicional trabalha principalmente ou quase exclusivamente também com a lógica dedutiva. O *Big Data* trabalha a partir de uma lógica indutiva de

---

[103] GONÇALVES, Maria Eduarda - *The EU data protection reform and the challenges of big data*: *remaining uncertainties and ways forward*, p.11 [Em linha]. [2017]. [Consult. 6 out. 2018]. Disponível em WWW:<URL:https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1295838>.

[104] Posição pela negociação *ad hoc*, frente aos dados provenientes de *Big Data.* QUELLE, Claudia – *Not just user control in the General Data Protection Regulation*. *On controller responsibility and how to evaluate its suitability to achieve fundamental rights protection*, p.3 [Em linha]. [2011]. [Consult. 10 out. 2018]. Disponível em WWW:<URL:https://pdfs.semanticscholar.org/2eeb/f1efca870fc524b381010c97712f98e89419.pdf> .

[105] SKYRMS, Bryan - **Escolha e acaso**. São Paulo: Cultrix, 1966, p. 11.

[106] REICHENBACH, Hans - ***Erfahrung und Prognose***. Wiesbaden: Springer Vieweg, 1983, p. 212.

[107] SKYRMS, Bryan - **Escolha e acaso**. São Paulo: Cultrix, 1966, p. 16-17.

dados, para que possa encontrar com agilidade uma análise de correlações para o reconhecimento de padrões futuros.

Com referência aos critérios aludidos, a melhor forma de se ter os conceitos bem definidos é através do exemplo: imagine-se uma pessoa a conduzir um automóvel.

No caso do uso da lógica dedutiva, para a pessoa que possui um automóvel com condução autónoma, este pode medir as variáveis de velocidade dos peões, o tempo em que o semáforo trabalha, a distância a percorrer, as variáveis de velocidade dos outros carros e para isso tudo vai utilizar cálculos. Desta forma, os argumentos são dedutivamente válidos e verdadeiros. Nota-se que é um processo lento para uma pessoa normal realizar e despende de energia do condutor nos casos de uma condução normal.

No caso do uso da lógica indutiva e considerando a mesma situação, o condutor de automóvel normal não possui de tempo suficiente e nem de informação suficiente para analisar os dados até a chegada ao semáforo, o cérebro dele consegue processar as informações num contexto global de forma indutiva, baseado em generalização de probabilidade de situações similares, o cérebro processa as informações mais importantes.

A questão do risco inerente à análise de *Big Data*, é marcada pelo uso da lógica indutiva. Valendo-se da agilidade do tráfego dos dados na internet, com o objetivo de extrair informações úteis, foi necessário recorrer ao uso de tal lógica.

A lógica indutiva é o oposto da dedutiva, que é a forma clássica e a mais conhecida. Aquela não teria a capacidade para analisar os dados que são gerados a cada segundo devido à velocidade de processamento necessária. Sendo assim, a lógica indutiva foi a alternativa mais viável para análise satisfatória, via *Big Data*, para obter correlação ou padrões de previsibilidade (FLORIDI, 2012).

Por todos esses aspetos, o *Big Data* pode resultar em riscos de informações não verdadeiras, principalmente porque tratamento de dados é realizado através da lógica indutiva.

3.4.2 Encarregado da Proteção de Dados (EPD)

Dentro do contexto de AIPD, impõe-se expor a figura do Encarregado da Proteção de Dados[108] (doravante EPD). Muito comumente, em inglês, chamado de *DPO* (*Data*

[108] Art.º 37.º ao 39.º do RGPD.

Protection Officer), figura que em alguns países da União já existia[109] antes do RGPD, porém, em Portugal é uma figura nova.

Por força da natureza, âmbito ou finalidade dos dados que tenham origem em larga escala[110], onde se encaixam os dados do *Big Data*, e que requeiram um esfoço maior de controlo constante e sistemático, ficam o RT e o subcontratante (se existir) responsáveis sempre pela designação de um EPD[111]. A referida nomeação deverá ser realizada nos casos em que o RT ou o subcontratante tenham como atividades principais[112], o tratamento de dados em larga escala[113] (*Big Data)*, que sejam de categorias especiais de dados pessoais[114], dados pessoais que tenham relação com condenações penais e infrações[115], entre outros.

A abordagem ora relacionada na presente dissertação, é especificamente direcionada para os dados pessoais que tenham como fonte *Big Data*. Desta forma, é importante a leitura do Art.º 37.º do RGPD, que relaciona todas as demais[116] hipóteses em que sempre o RT e o subcontratante designam um EPD.

---

[109] A figura do EPD já era recomendada antes da entrada em vigor do RGPD, segundo GT29 quanto as orientações da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, adotadas em 13 de dezembro de 2016 e revistas em 5 de abril de 2017.

[110] Sobre o pré-requisito da definição de larga escala constante no Regulamento. Grupo de Trabalho do Artigo 29.º - Orientações sobre os encarregados da proteção de dados (EPD) (16/PT WP 243 rev.01). p.7 [Em linha]. [2017]. [Consult. 7 out. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf>.

[111] Artigo 37.º, b) e c) do RGPD.

[112] Segundo o Grupo de Trabalho do Artigo 29.º a definição de "As «atividades principais» podem entender-se como as operações essenciais para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, as quais incluem também todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante. Por exemplo, o tratamento de dados relativos à saúde, designadamente os registos de saúde dos doentes, deve ser considerado uma das atividades principais de qualquer hospital, pelo que os hospitais devem nomear EPD. Por outro lado, todas as organizações exercem determinadas atividades de apoio, nomeadamente a remuneração dos seus trabalhadores ou atividades comuns de apoio informático. Trata-se de exemplos de funções de apoio necessárias para a atividade principal ou a área de negócio central da organização. Embora sejam necessárias ou essenciais, por norma estas atividades são consideradas funções acessórias e não a atividade principal". *Idem*, p. 23.

[113] Em larga escala, segundo o Considerando 91: "Tal deverá aplicar-se, nomeadamente, às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados…" claramente se pode chegar a conclusão de que os dados obtidos via *Big Data* está incluído na nova tecnologia em que o Considerando aponta.

[114] Art.º 9.º do RGPD.

[115] Art.º 10.º do RGPD.

[116] Todas as hipóteses que é obrigatória as nomeações de um EPD estão previstas no artigo 37.º, n.º 1, a), b) e c) do RGPD.

3.4.3 Características do Encarregado da Proteção de Dados

O EPD tem como características principais a independência e a confiabilidade, com obrigação de sigilo e o controlo em conformidade com o RGPD. O sucesso da Abordagem Baseada no Risco é fruto também de contribuição ativa do EPD. Sempre que houver operações de tratamento de dados pessoais o EPD possui como funções:

- Informações;

- Aconselhamento;

- Controlo e

- Reporte de informações.

O mesmo pode ser um funcionário da empresa ou ser externo à esta, possui um estatuto e funções próprias. Como auxílio para desempenho das suas funções, pode-se valer da ajuda do RT e/ou do subcontratante. Tem o dever de informar, aconselhar e fiscalizar o cumprimento do RGPD, sendo uma ponte de contacto diretamente com a Autoridade de Controlo[117].

Cumpre salientar que o EPD é um colaborador ativo para o êxito da Abordagem Baseada no Risco. É ele quem realiza a análise minuciosa dos riscos nas operações de tratamento de dados pessoais.

As empresas devem garantir que o EPD seja convidado a estar presente em todas as reuniões dos quadros de gestão médios e superiores sempre que estejam envolvidas decisões relacionadas com proteção de dados. Todas as informações importantes devem ser comunicadas ao EPD, para que este possa prestar um aconselhamento direcionado para cada caso específico, devendo o parecer do mesmo ser sempre observado.

Em caso de desacordo com o EPD, o GT29 recomenda, que sejam justificados os motivos para não seguir o parecer do mesmo[118]. Este deverá imediatamente ser consultado após a ocorrência de uma suposta violação de dados ou outro incidente.

Segundo o Art.º 39.º, n.º 2: "No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento,

[117] Art.º 37.º, 38.º e 39.º do RGPD.
[118] Sobre as funções do EPD. V. Grupo de Trabalho do Artigo 29.º - Orientações sobre os encarregados da proteção de dados (EPD) (16/PT WP 243 rev.01). p.7 [Em linha]. p.17 [2017]. [Consult. 7 out. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf>.

tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento". Após a avaliação dos riscos relacionados, ainda deverá fazer uma seleção dos dados que apresentam riscos ainda mais elevados. O EPD deve possuir quatro tipos de proteções:

- Independência;

- Não lhe pode ser dado o modo de execução das tarefas a realizar;

- Não pode ser penalizado pelo exercício da função e

- Não pode ser destituído pelo exercício da função.

Nos casos de trabalhadores subordinados, sendo o mesmo do RT ou do subcontratante, deve ser assegurado:

- A autonomia técnica para o exercício das funções de acordo com Art.º 116.º do Código do Trabalho;

- Para a penalização pelo exercício das funções enquanto encarregado, qualquer sanção disciplinar aplicada deve ser considerada sanção abusiva de acordo com o Art.º 331.º do Código do Trabalho e

-Deve ser assegurada a proteção contra o despedimento, presumir sem justa causa o mesmo (SILVA, 2018).

Levando em consideração os aspetos citados, o EPD deve realizar as funções que lhe são inerentes de forma autónoma. Só desta maneira o RGPD é aplicado de forma correta e se assegura a imparcialidade nas tomadas de decisões nos casos de se tratar de um EPD que é um trabalhador subordinado.

3.4.4 O EPD e o Subcontratante

As empresas que preenchem os critérios de designação obrigatória do EPD[119] , fazem-no por força de lei. Mas isto não obriga a contratação de um EPD pelo subcontratante. Da mesma forma, quando o subcontratante for obrigado a constituir um EPD, a empresa não é obrigada a também cumprir essa medida.

[119] Art.º 37.º do RGPD

De uma forma muito elucidativa, imagina-se a seguinte situação[120]: existe uma empresa de pequena dimensão e familiar, que tem como atividade principal a distribuição de eletrodomésticos, em espaço único de entrega. Contrata um subcontratante com a finalidade de prestação de serviços analíticos, controlo do sítio da *web*, publicidade e marketing direcionado.

A empresa não realiza um tratamento de dados em larga escala, uma vez que é de pequena dimensão. Porém, se o subcontratante possui uma ampla rede de contactos, apenas o subcontratante preenche os critérios do Art.º 37.º, n. º1, alínea b) do RGPD. E deve, desta forma, designar um EPD. O mesmo EPD faz a supervisão de todas as atividades realizadas pela organização do subcontratante, nos casos em que este atuar na qualidade de RT, *v.g.* recursos humanos, informática e logística. A pequena empresa, que não preenche os critérios, não é obrigada a designação do mesmo.

Pode-se observar que a função do EPD é de grande responsabilidade tendo como característica principal a aplicação correta do RGPD, mas não ficando obrigada a sua nomeação nos casos em que o subcontratante preencher os requisitos e a empresa contratante não preencher os mesmos.

3.4.5 A Localização do EPD

Deverá ser observado com coerência o sistema a ser adotado, dado que é de suma importância a localização do EPD, que deve favorecer a fácil acessibilidade do mesmo[121]. Na referida matéria, com a finalidade de atingir a melhor coerência para responder a todos os desafios, que são normalmente impostos ao direito, o GT29 recomenda que o EPD deverá estar dentro da União, independente da localização do RT ou o subcontratante. Porém, seria mais aceitável, para desenvolvimento das suas funções com êxito, que o EPD esteja localizado nas proximidades do RT e do subcontratante.

Dado o exposto, para que o EPD possa desenvolver um trabalho eficaz, é aceitável a sua localização fora da União, perto do RT e do subcontratante[122].

---

[120] *Idem*, p 11. Caso prático idealizado pelo Grupo de Trabalho do Artigo 29.º
[121] Segundo secção 4 do Regulamento do artigo 37, n. º2 do RGPD.
[122] Grupo de Trabalho do Artigo 29.º - Orientações sobre os encarregados da proteção de dados (EPD) (WP 243 rev.01). [Em linha]. [2016]. p. 10. [Consult. 5 dez. 2018]. Disponível em WWW:<URL: https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf>.

3.5 Abordagem Baseada no Risco e o Procedimento Posterior

Dentro do contexto *a posteriori*, no que toca o tratamento dos dados, por força do Art.º 33.º e 34.º do RGPD, existe a figura da Notificação da violação dos dados pessoais à autoridade de controlo e a Comunicação aos titulares dos dados.

O RGPD torna obrigatória a Notificação, nos casos de violação, para todos os RTs. Tal procedimento já estava presente na legislação europeia desde a Diretiva 2002/58/CE[123] do Parlamento Europeu e do Conselho, de 12 de julho de 2002, que tutelava à privacidade e as comunicações eletrónicas. Alguns Estados-Membros já regulamentavam a Notificação[124], quando estava em questão a violação de dados pessoais; porém noutros países, como Portugal, é uma novidade a ser implementada.

É geralmente reconhecida a complexidade no que se refere a segurança de dados pessoais. Mesmo que se tenha cautela no processamento, existe sempre a possibilidade de incorrer em violações[125]. Constatado esse perigo, o RGPD estabelece a obrigação da Notificação. Tal procedimento, deverá deixar algumas questões transparentes, como por exemplo, esclarecer os critérios de identificação das violações (especificando quanto à natureza da violação), o prazo, nome, os contactos do encarregado da proteção de dados, as consequências, entre outras.

Toda informação deverá estar disposta de forma rápida e esclarecedora no que toca as causas da violação, para que a Autoridade de Controlo possa fazer uma análise coerente e verificar o cumprimento do RGPD.

Prima facie, existe uma flexibilidade na questão da Notificação, dando liberdade e capacidade para que a Autoridade de Controlo seja informada de forma gradual[126], sem

[123] Grupo de Trabalho do Artigo 29.º - Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (18/PTWP250 rev.01) [Em linha]. [2017]. [Consult. 23 nov. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>.

[124] Atualmente, fica com a obrigação de notificar os casos de violação para algumas organizações, como por exemplo os fornecedores de serviços de comunicações eletrónicas acessíveis ao público, de acordo com a Diretiva 2009/136/CE e no Regulamento (UE) n.º 611/2013. Alguns Estados-Membros já possuem a sua própria obrigação interna a notificação da referida violação. Tal pode incluir a obrigação de notificar violações que envolvam categorias de responsáveis pelo tratamento, além dos fornecedores de serviços de comunicações eletrónicas acessíveis ao público, como exemplo os países: Alemanha e Itália, ou uma obrigação de comunicar todas as violações que envolvem todo o tipo de dados pessoais por exemplo os Países Baixos. Idem, p. 11.

[125] A definição de violações de dados pessoais está elencada no artigo 4.º, n.º 12 do RGPD, que diz: "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

[126] Art.º 33.º n. º 4 do RGPD.

demora injustificada. Sobre a comunicação entre o RT e a Autoridade de Controlo, deve ocorrer com dever de registo[127] das atividades de tratamento.

A finalidade da Notificação é que a Autoridade de Controlo tenha a oportunidade de se manifestar a respeito da violação, dar aconselhamento ao RT, indicando se há necessidade de Comunicação aos titulares dos dados ou não sobre a violação[128]. É o RT quem deve motivar a referida Notificação à autoridade de controlo.

É importante analisar a questão da frequência da Notificação, pois, poderá ser um ónus para o RT. Caso seja constatado volume e frequência rotineira, em que situações o RT deve ou não realizar a Notificação. O GT29 realizou um parecer[129] no ano de 2014, relativo a violação dos dados pessoais, que era direcionado à Diretiva 2002/58/CE, mas que permanece atual, onde oferece orientações aos RT no sentido de ajudar a decidir na questão da Notificação. O referido parecer é de suma importância, pois, traz exemplos e situações em que o RT é obrigado a realizar a Notificação e a Comunicação[130].

Os casos relacionados com a tecnologia *Big Data*, são fortes candidatos a serem analisados *a posteriori*, pois apresentam todas as características de elevados riscos para os direitos e liberdades das pessoas singulares, dado que muitas vezes, mesmo tendo em consideração a Avaliação de Impacto Prévia sobre a Proteção de Dados, tal não basta para evitar indesejáveis violações.

Muito mais além vai o RGPD em matéria de violação de dados, que tem como pano de fundo assegurar esses direitos fundamenteis, em especial nos casos de *Big Data*. Prevê o Art.º 34.º, n.º 1 da mesma norma, que deverá ser realizada a Comunicação para os titulares dos dados que foram violados, sempre que estiver em causa um elevado risco para os direitos e liberdades individuais. Isto posto, vê-se duas atitudes (*a posteriori*) a serem realizadas pelo RT: uma é a Notificação, já referida anteriormente e a outra é a Comunicação.

---

[127] Art.º 30.º do RGPD.
[128] Disposto no artigo 34.º, n.º 4, e artigo 58.º, n.º 2, alínea e) do RGPD.
[129] Grupo de Trabalho do Artigo 29.º - Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (18/PTWP250 rev.01) [Em linha]. [2014]. [Consult. 15 out. 2018]. Disponível em WWW:<URL:http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf>.
[130] *Idem*, p.6.

A finalidade da Comunicação é dar o conhecimento e a oportunidade às pessoas, que tiveram os seus dados violados, os meios adequados para se protegerem das consequências que poderão sofrer, principalmente as de carácter de dano reputacional.

Como se observa, o papel do RT é um fator importante, que merece destaque, para alcançar o sucesso da aplicabilidade do RGPD, colaborando de forma ativa e com grande responsabilidade. O mesmo, caso não realize as referidas Notificações e/ou Comunicações, incorre em possível sanção[131].

Levando em consideração que os dados provenientes de *Big Data* são fortes candidatos para esse tipo de questão, podem estar em tela situações que obrigam à Comunicação a elevado número de pessoas e de forma frequente, ficando o RT com o encargo de tal medida. Nos casos em que fique comprovado que tal exija um esforço desproporcional, pode ser realizada a comunicação pública[132] ou outra medida semelhante e com o mesmo efeito.

Deverão ser juízo de valor do RT, a análise dos critérios que identifiquem uma violação e baseado neles, justifique que o mesmo realize a Comunicação aos titulares. Desta forma, o RT ao detetar o que seja uma violação que possa implicar um elevado risco, deverá impulsionar a Comunicação.

Quando existe perda de controlo dos dados pessoais, limitação de direitos, discriminação, furto ou usurpação de identidade, perdas financeiras, inversão de pseudonimização quando não autorizada, danos à reputação da pessoa, no caso do sigilo profissional a perda da confidencialidade, ou quando se mostrar situações de desvantagem no aspeto económico ou social para os titulares dos dados[133], podem existir danos físicos, materiais ou imateriais.

Posto isto, o RT deverá fazer uma análise dos eventuais danos e o reflexo nas vidas das pessoas.

O RGPD deve salvaguardar Direitos Fundamentais, no entanto deixa algumas dúvidas sobre se possui a capacidade de acompanhar a evolução tecnológica e tutelar os princípios e direitos norteadores da proteção de dados. Além do que já foi relatado na presente dissertação, importa ressaltar que com o atual grau de recolha e tratamento de dados,

[131] Em relação a condições gerais para a aplicação de coimas no Art.º 83.º do RGPD.
[132] Ver Art.º 34.º, n. º3, alínea c) do RGPD.
[133] Considerando 85 do RGPD. Nos casos em que o responsável pelo tratamento deverá fazer um juízo de valor nos danos e reflexo na vida dos titulares dos dados, caso não sejam adotadas medidas adequadas e oportunas, quando ocorra a violação de dados pessoais.

principalmente ligados à internet e em que é de fácil identificação do utilizador, fica ainda por responder se o RGPD, mesmo utilizando a autorização prévia, a limitação de finalidades e a minimização de dados, tal bastará[134] para resguardar às finalidades para as quais foi criado.

3.6 Abordagem de Autodefesa

A abordagem de autodefesa tem como objetivo fechar o ciclo da abordagem baseada no risco. Será como se fosse uma fase que completa a ideia inicial.

O reflexo da violação de dados, seja de qualquer ordem for, será provavelmente, inicialmente sentido pelos titulares dos dados e não necessariamente pelo RT. Partindo deste princípio, a abordagem de autodefesa revela-se para o escopo do RGPD como o poder de reação atribuído ao titular dos dados, sempre que estiver em causa violação de dados, o tratamento não autorizado, o elevado risco e o tratamento indesejado.

Mais uma vez se impõe a importância das funções do RT, sendo neste caso o dever de informação.

Os deveres de informação do RT aos titulares dos dados preza pela transparência, para que possa ser evitado ou minimizado qualquer consequência negativa para os mesmos. Configura um direito destes, de terem conhecimento de onde e como os seus dados estão a circular no "mundo virtual" e real. A Comunicação deverá ser de forma concisa, transparente, inteligível e de fácil acesso. A informação deverá ter forma escrita tradicional ou mesmo por meios eletrónicos e também poderá ser de forma oral, sempre que for solicitado pelos titulares[135].

Apesar de se apresentar como um importante meio de defesa, somente terá eficácia se a informação for seguida como regra e habitualidade pelo RT.

A sociedade atual é acelerada, e os meios eletrónicos utilizados com frequência, pelo que seria impossível aos titulares dos dados reagirem em oposição a qualquer tratamento em que não tenham ciência que está a ser realizado. A informação oferecida pelos RTs evita que os utilizadores sejam informados apenas quando um dano já esteja na esfera jurídica.

---

[134] GONÇALVES, Maria Eduarda - *The EU data protection reform and the challeges of big data*, p. 3,13 e 14 [Em linha]. [2017]. [Consult. 21 out. 2018]. Disponível em WWW:<URL: <https://www.tandfonline.com/doi/pdf/10.1080/13600834.2017.1295838?needAccess=true>.

[135] Art.º 12.º do RGPD - Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados.

3.7 Autodeterminação Informacional

Aos titulares dos dados são conferidos instrumentos que têm como finalidade resguardar a autodeterminação informacional dos mesmos. No sentido de elucidar a origem da ideia de autodeterminação informacional, que norteia a Abordagem de Autodefesa, é necessário citar o Tribunal Federal Constitucional Alemão. O Tribunal, ao analisar um processo[136] que rezava sobre informações que foram recolhidas das pessoas durante o senso de 1983, levou em consideração o processamento moderno da época, visando uma maior proteção para as pessoas, no que toca a recolha, armazenamento, uso e divulgação de forma ilimitada dos dados pessoais, sendo assim, abrangido pelos direitos gerais das pessoas. Tais direitos estavam garantidos na Constituição alemã como direitos fundamentais. Desta forma, as pessoas teriam uma capacidade maior de decidir a respeito do uso e divulgação dos seus dados pessoais. Apenas o interesse público imporia limitações à autodeterminação informacional.

A doutrina portuguesa[137] rececionou a autodeterminação informacional no seu Art.º 35.º da Constituição portuguesa, conseguindo desta maneira proteger uma amplitude de direitos fundamentais, impedindo a transformação das pessoas em objeto/fonte de informação remunerada.

O direito de autodeterminação informacional é: *"el control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas*"[138] [139].

Da autodeterminação informacional emanam três direitos[140], são eles:

- Acesso dos titulares dos dados a todos os registos informáticos que lhes digam respeito, bem como a sua retificação e a complementação dos mesmos;
- O sigilo referente aos responsáveis de ficheiros automatizados e o direito à sua não interconexão e
- O não tratamento informático de alguns tipos de dados pessoais.

---

[136] SCHWABE, Jürgen - Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. [Em linha]. [2006]. [Consult. 21 nov. 2018]. Disponível em WWW:<URL:https://www.kas.de/c/document_library/get_file?uuid=c0b3d47d-beba-eb55-0b11-df6c530ddf52&groupId=252038>.

[137] CANOTILHO, José Gomes e MOREIRA, Vital - **Constituição da República Portuguesa - Anotada** - Volume I - Artigos 1º a 107º. Coimbra: Coimbra Editora, 2014, p.553.

[138] CUEVA, Pablo Lucas Murillo de la e MANÃS, José Luís Piñar - ***El derecho a la autodeterminación informativa, Madrid, Fundación Coloquio Jurídico Europeo***, 2009, pág. 11.

[139] PINHEIRO, Alexandre Sousa - ***Privacy* e proteção de dados pessoais: a construção dogmática do direito à identidade informacional**. Lisboa: AAAFDL, 2015, pág. 803.

[140]CANOTILIO, José Gomes e MOREIRA, Vital - **Constituição da República Portuguesa - Anotada** - Volume I - Artigos 1º a 107º. Coimbra: Coimbra Editora, 2014, p.551.

Para além dos direitos e princípios que coroam a matéria em questão, o facto da igualdade[141] tem uma forte presença em tela, pois, todas as pessoas precisam estar no mesmo patamar de igualdade para que se possa reagir ao eventual tratamento de dados pessoais, de forma positiva ou não[142]. A igualdade entre pessoas é sinónimo de justiça, o que também contribui para os fins do RGPD.

A Abordagem de Autodefesa possui, como aliado, um princípio que é o da transparência.

O princípio da transparência vem plasmado no RGPD e postula que deverão ser tomadas medidas adequadas pelo RT ao comunicarem com os titulares dos dados, de forma concisa, transparente, inteligível e de fácil acesso, com uma linguagem clara e simples, atenção redobrada nos casos em que as informações são direcionadas para as crianças[143]. Observa-se que o princípio da transparência é um princípio geral em matéria de proteção de dados e que se encontra nos Art.º s 12.º ao 15.º da norma.

Não obstante o princípio da transparência se encontrar devidamente regulamentado, poderá ser questionado a ininteligibilidade das pessoas em relação aos algoritmos, devido a complexidade da lógica relacionada com o *Big Data*.

Segundo o Art.º 13.º, n. º2, alínea *f)* do RGPD deverá ser apresentado da seguinte forma: "informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados". Assim, fica o RT com a função de fornecer informações que sejam úteis e com a clareza que a matéria obriga. As informações deverão ser úteis, isso significa que deverão ser explicadas de forma que todas as pessoas possam entender. Desta forma o RT deverá criar meios para que consiga transformar determinada informação e transmitir de maneira o mais acessível que for possível.

Neste sentido, defende-se o direito à explicação[144], para que as pessoas possam ter conhecimento do facto e compreendê-lo, terem consciência que os resultados de uma análise proveniente de técnicas de *machine learning* (por exemplo), possa ter reflexo de carácter discriminatório nas vidas das pessoas.

---

[141] MENDES, João Castro - **Direito Comparado**. Lisboa: AAFDL,1983, p. 335.

[142] CLARO, João Martins - **O Princípio da Igualdade, *in* Nos Dez Anos da Constituição**, obra coletiva. Lisboa, 1987, p. 31.

[143] Art.º 12.º, n. º 1 do RGPD.

[144] Sobre o direito à explicação ver WACHTER, Sandra - *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. [Em linha]. [2017]. [Consult. 12 jan. 2019]. Disponível em WWW:<URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469>.

Dito o exposto, a Abordagem de Autodefesa é então um direito oferecido aos titulares dos dados pessoais pelo RT, para que por meio da autodeterminação informacional, possam ter o controlo e domínio dos seus dados pessoais. Os titulares podem solicitar informações claras, que permitam o perfeito conhecimento e compreensão da matéria a seu respeito.
Dessa forma, o direito à autodeterminação informacional é reconhecido e assume realce no domínio do tratamento dos dados pessoais. Assim visa proteger a privacidade, não deixando de salientar que o referido direito flanqueia e alarga a tutela dos direitos fundamentais da liberdade de comportamento e da privacidade[145], após a revisão constitucional de 1997, que veio consagrar expressamente o direito de cada pessoa de traçar o seu próprio plano de vida, sendo o direito de livre desenvolvimento da personalidade[146].
A autodeterminação informacional faz parte de um direito que atribui a cada cidadão o direito de ser ele próprio, decidindo quando e os limites que os seus dados pessoais podem ser revelados.

CAPÍTULO IV - O CONSENTIMENTO

O Consentimento[147] para o tratamento dos dados pessoais ganha uma grande valorização no RGPD na tutela dos direitos da proteção das pessoas. Não menos importante é evidenciar também que existem outros fundamentos para o tratamento legítimo dos dados pessoais previsto por lei, porém o que será explorado é o Consentimento que não sofre imposição legal para a sua aplicação, e que oferece legitimidade para o tratamento de dados pessoais de forma legal e lícita.
Convém, antes de tudo o mais, citar o considerando 32 do RGPD sobre o Consentimento dos titulares dos dados. Este descreve a forma como o manuseamento dos dados pessoais deve ser realizado, uma vez que os dados pertencem às pessoas e não às empresas.
O Consentimento dos titulares dos dados deverá seguir o RGPD na sua literalidade, onde se encontram palavras que devem ser analisadas para se realizar o verdadeiro Consentimento, sendo elas:
- Ato positivo;
- Claro;

[145] Acórdão do Supremo Tribunal de Justiça no processo número 679/05.7TAEVR.E2. S1 de 16-10-2014. Em relação à autodeterminação informacional.
[146] Acórdão do Tribunal Constitucional no processo n.º 288/98, in, 40.º vol., pág. 61. Sobre a Autodeterminação informacional.
[147] Nos termos do n.º 11, do art.º 4º, do RGPD: "«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;"

- Vontade livre;

- Específica;

- Informada e

- Inequívoca.

Estas palavras não deixam a mínima dúvida quanto às finalidades do uso dos dados pessoais, estes também derivados de *Big Data*, consequentemente sujeitos ao RGPD e apresentando maior dificuldade para o tratamento, sendo aplicável também aos formatos eletrónicos.

Os titulares podem manifestar uma vontade positiva para o tratamento dos seus dados, quando ao navegar num sítio na internet, optam pela validação de uma opção apresentada ou também ao preencher uma declaração ou outra ação que indique a vontade de permitir o tratamento dos seus dados[148].

Considerando a hipótese do silêncio, antes era habitual nas relações com os utilizadores, estes serem confrontados com sítios na internet que propunham no sentido de não preenchimento dos campos de autorização para tratamento de dados, sendo tal considerado como permissão para o uso dos mesmos. Agora com o RGPD, ao contrário da situação anterior, a autorização deve ser de forma positiva. O Consentimento deixou de ser válido nos casos do silêncio segundo Calvo (2017, p. 120).

Dado o exposto, o Consentimento entra no cenário atual como sendo um quesito de grande importância para que o tratamento de dados pessoais seja considerado lícito, não se podendo também descurar outras formas de fundamento legítimo previsto em lei (no próprio RGPD, direito da União, direito de um Estado-Membro, obrigações legais que o RT deve cumprir ou a realização de contratos em que o titular dos dados seja parte)[149].

O Consentimento tem como característica encontrar-se no eixo central das normas sobre a proteção de dados, sendo causa principal de tratamento de dados pessoais[150], cabendo aos titulares dos dados decidir[151] o destino e porque os seus dados serão tratados. Este poder de decidir é fruto decorrente do direito à autodeterminação informacional.

Para que o RGPD seja um instrumento que vem colaborar com as finalidades ora propostas, é admissível que o Consentimento, nos casos em que foi dado antes da entrada em vigor da legislação

---

[148] Exemplos do Considerando 32 do RGPD.

[149] Considerando 40 do RGPD.

[150] CORDEIRO, António Barreto Menezes - O consentimento do titular dos dados no RGPD. [Em linha]. [2018]. [Consult. 24 jan. 2019]. Disponível em WWW:<URL:https://blook.pt/publications/publication/e772e2d8f7b4/>.

[151] MARCOS, Isabel Davara Fernández de - ***Hacia la estandarización de la protección de datos personales: Propuesta sobre una «tercera vía o tertium genus» internacional***. Madrid: La Ley, 2011, p.145.

possa ter validade depois, com a condição de que estejam a ser cumpridas as regras previstas no RGPD[152].

Incidindo esta dissertação nos efeitos nas relações jurídicas de dados originados via *Big Data*, cabe reflexão nos casos de situações em que aparentemente o Consentimento pode ser considerado válido à luz do RGPD, mas de facto não é, passando a remota impressão de que as pessoas possuem o controlo dos seus dados pessoais, nas seguintes situações[153]:

-Quando a recusa do Consentimento resultar em sérios danos;

-Quando o Consentimento for solicitado por um superior hierárquico ou

-Quando é necessário para a pessoa ter acesso a bens e serviços indispensáveis à vida.

Desta forma o Consentimento possui um verdadeiro canal de angariar autorizações para o uso, recolha e tratamento de dados pessoais, possuindo um efeito contrário do que está disposto no RGPD.

Afigura-se importante focar que, os aplicadores do direito devem estar atentos para que não se desvirtue a letra da lei e os seus objetivos.

O Consentimento é a resposta mais adequada para esta dissertação, sendo a forma mais segura que permite que os utilizadores percebam que os dados pessoais são algo que lhes pertençam, e não como estão acostumados a ver, quando as empresas os utilizam como se fossem os verdadeiros proprietários.

Atualmente, o Consentimento deve ser de forma clara e concisa, isto é, não cabe mais a prática de enviar um longo texto, com pequenas letras e preenchido por defeito, como era a prática antes da entrada em vigor do RGPD. A linguagem deverá ser de fácil inteligibilidade[154], sendo oferecido de forma que se consiga distinguir dos termos e condições.

O pedido para o Consentimento deverá respeitar os seguintes requisitos:

- Manifestação de vontade[155] livre, específica, informada e explícita[156];

---

[152] Comissão Europeia - O consentimento dado antes de 25 de maio de 2018 continua a ser válido quando o RGPD passar a ser aplicável a partir de 25 de maio de 2018? [Em linha]. [2018]. [Consult. 14 jan. 2019]. Disponível em WWW:<URL:https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_pt>.

[153] Ao citar Spiros Simitis. CORDEIRO, António Barreto Menezes - O consentimento do titular dos dados no RGPD. [Em linha]. [2018]. [Consult. 24 jan. 2019]. Disponível em WWW:<URL:https://blook.pt/publications/publication/e772e2d8f7b4/>.

[154] Grupo de Trabalho do Artigo 29.º - Sobre a prestação mais harmonizada da informação (11987/04/PT GT100), p. 10. [Em linha]. [2016]. [Consult. 5 dez. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf >.

[155] Sobre a manifestação de vontade é importante ressaltar que, não se pode confundir com o Consentimento em si. Sendo a mesma integrante dos requisitos formadores do Consentimento. Desta forma, considera-se o Consentimento como um entendimento amplo. CORDEIRO, António Menezes - **Tratado de Direito civil** II. Almedina: Coimbra, 2014, p.123.

[156] Art.º 4.º, n. º 11 do RGPD.

- O RT ter a possibilidade de demonstrar que foi dado Consentimento validado[157];

- A possibilidade de os titulares dos dados poderem retirar o seu Consentimento a qualquer altura[158];

- O Consentimento de menores de 16 anos está dependente de autorização dos titulares da responsabilidade parental[159] e

- Os Consentimentos de dados sensíveis são categorizados como dados que merecem cautelas no tratamento, pois são classificados como de risco elevado[160].

Com a obrigatoriedade de obtenção do Consentimento, vem como consequência o aumento e a agravação dos deveres do RT, sendo este quem deve ter a obrigação de informação aos titulares dos dados, o que também obriga a que seja realizado um controlo maior por parte das entidades de supervisão.

4.1 Manifestação de Vontade Informada

A informação é o pressuposto do Consentimento informado. O titular dos dados pessoais deverá ter conhecimento prévio[161] do tratamento de dados assim como das suas finalidades.

O Consentimento informado significa que deverá ser esclarecido aos titulares dos dados pessoais da seguinte forma:

- A identidade de quem vai tratar os dados;

- Os fins do tratamento;

- Quais os tipos de dados que serão tratados;

- A existência da possibilidade da retirada do Consentimento;

- A possibilidade de os dados serem tratados e utilizados por decisões automatizadas e

- A possibilidade de o Consentimento resultar em transferência internacional dos dados pessoais, os riscos de estarem fora do espaço da União Europeia[162] [163].

Tendo em vista os aspetos observados, não é válido o Consentimento que é apresentado às pessoas onde as caixas das alternativas já estejam marcadas. Se os utilizadores não desmarcarem as alternativas que aceitam o tratamento dos seus dados pessoais, por não se aperceberem, este

[157] Art.º 7.º, n. º 1 do RGPD.
[158] Art.º 7.º, n. º 3 do RGPD.
[159] Art.º 8.º, n. º 2 do RGPD.
[160] Art.º 9.º do RGPD.
[161] O facto de ser prévio faz todo o sentido, pois, somente sendo fornecida a informação e analisada pelos titulares dos dados, é que estes podem fazer um juízo sobre a possibilidade do tratamento.
[162] Art.º 6.º e 7.º e considerandos 42 e 43 do RGPD.
[163] Grupo de Trabalho do Artigo 29.º - Orientações relativas ao Consentimento na aceção do Regulamento (UE) 2016/679 (17/PTWP259 rev.01) [Em linha]. [2017]. [Consult. 18 dez. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf >.

Consentimento à luz do RGPD não é considerado válido, porque as opções pré-validadas não são válidas.

O Consentimento é o meio pelo qual as pessoas possuem para escolher a respeito do tratamento dos seus dados pessoais que emana de um direito que faz parte não somente do RGPD, como está integrado na Carta dos Direitos Fundamentais da União Europeia, como direito fundamental de terceira geração, devido a nova realidade que vive a sociedade atual, que ganhou força de natureza vinculativa em 2009 no Tratado de Lisboa[164].

A Carta dos Direitos Fundamentais da União Europeia[165] está dividida em:

- Dignidade;
- Liberdades;
- Igualdade;
- Solidariedade;
- Cidadania e
- Justiça.

Dentro dos 54 artigos que formam o diploma, encontram-se direitos fundamentais como:

- Direito à Vida;
- Liberdade de Expressão;
- A Presunção de Inocência;
- O Princípio da Não Discriminação;
- Direitos Económicos e Sociais (proibição do trabalho infantil, saúde, educação, o direito de denunciar o trabalho de forma coletiva);

Constam também os direitos fundamentais de terceira geração que tutelam as novas realidades que são:

-A Proteção dos Dados Pessoais;
- A Defesa do Consumidor;
- Proteção do Ambiente e
- O Desenvolvimento Sustentável.

Assim, o Consentimento está incluído na Proteção dos Dados Pessoais por constituir um direito fundamental em que assentam os princípios da Democracia e do Estado de Direito.

[164] Assembleia da República - Tratado de Lisboa. [Em linha]. [2008]. [Consult. 30 dez. 2018]. Disponível em WWW:<URL:https://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf >.
[165] Baseado na Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01).

Em relação às crianças[166], o Consentimento será lícito se elas tiverem pelo menos 16 anos. É dada a alternativa para os Estados-Membros dispor idade inferior, não podendo ser menor de 13 anos.

Atualmente, com o desenvolvimento de serviços tecnológicos cada vez mais ágeis, as pessoas têm um nível de exigência mais elevada em todos os sentidos, incluindo o Consentimento. A leitura das cláusulas não é inspiradora para a maioria dos utilizadores. Seja porque são longas, de difícil perceção ou por falta de paciência, o facto é que as pessoas não litigam na hora de aceitar algum serviço na *web*. Atualmente para uma pessoa aderir alguns serviços precisariam dispor de tempo e inteligibilidade suficiente para aceitar ou questionar determinadas imposições, como exemplo se pode verificar através de exemplos do tempo que levaria a ler as cláusulas de vários serviços na internet, em minutos (com velocidade de 250 palavras por minuto):

- Instagram: 50 min 4 seg;
- Google: 50 min;
- Facebook: 45 min 2 seg;
- Twitter: 44 min 7 seg;
- Snapchat: 42 min 3 seg;
- WhatsApp: 38 min;
- Apple iOS: 31 min 9 seg e
- Windows 10: 29 min 7 seg[167].

Desta forma uma pessoa precisaria de 4 horas e 5 minutos para conseguir finalizar a leitura de todo conteúdo disposto nas várias ofertas, levando em consideração que não existiriam dúvidas. Assim, chega-se a conclusão de que o Consentimento não pode ter a forma de cláusulas contratuais, deve ser realizado da forma mais simples possível para que as pessoas tenham disposição para uma leitura dinâmica.

Foram realizados estudos comportamentais e económicos sobre a realidade da Internet, onde resulta que a maioria das pessoas não leem as condições *online*, não tem capacidade ou conhecimentos para compreender a leitura (Menezes Cordeiro, 2019).

O Instituto de Pesquisa de Segurança Cibernética, localizada em Londres (agência europeia Europol), em colaboração com a empresa que patrocinou o estudo a *F-Secure*, realizou uma pesquisa que tinha como objetivo analisar o desconhecimento do público sobre as questões de segurança relacionada ao uso de internet *Wi-Fi.*

---

[166] Art.º 8.º do RGPD.

[167] Folha de São Paulo - Leitura de 'termos e condições' de serviços na internet exige 4,5 horas. [Em linha]. [2017]. [Consult. 9 jan. 2019]. Disponível em WWW:<URL:https://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-condicoes-de-servicos-na-internet-exige-45-horas.shtml>.

Foi elaborado um contrato em que continha a "cláusula de Herodes", que fazia referência ao rei da Judeia. Herodes teria ordenado a execução de todas as crianças que pudessem colocar o seu trono em causa. Assim, para que a pessoa pudesse ter acesso à rede *Wi-Fi*, deveria concordar e entregar o seu primeiro filho. O resultado da pesquisa foi a desativação da rede, depois que 6 londrinos aceitaram a cláusula, estando em espera mais 33 pessoas. Ficou comprovado que as pessoas não lêm os contratos *online*. É importante esclarecer que, como seria de se esperar, a referida cláusula é nula por ser contrária a todos os princípios de Direito e Justiça[168].

Logo, para que o Consentimento seja exercido de forma plena e efetiva na vida das pessoas, deve-se estar preparado para lidar com os meios tecnológicos, a começar pela leitura que é proposta no ato da adesão de serviços *online,* em especial os gratuitos. A maioria das pessoas talvez não estejam preparadas de forma preventiva para exercer a tutela dos seus dados pessoais[169]. O Consentimento deverá ser realizado de forma cautelosa, pois, o que está em causa é o destino dos dados pessoais de cada indivíduo, sendo a proteção destes uma questão fundamental da era digital atual, tendo em conta a relevância jurídica invasiva.

Sendo certo que, o Consentimento não está e nem poderia ser regulado exclusivamente pelo RGPD, pois fala-se em regime negocial que é regulado pelo Código Civil, para além de todos os pré-requisitos que formam um Consentimento válido, encontra-se com maior relevância a figura da manifestação de vontade, que somente na esfera civilística se poderá conseguir amparo legal de todo o regime negocial que exige este item (A. Barreto Menezes, 2018).

Cabe aos aplicadores do direito, recorrer ao regime do Negócio Jurídico[170], devendo ser realizada a adaptação adequada ao RGPD, nos casos em que este não apresente uma solução especial. Sendo certo que sempre será de aplicação o direito Comum quando a norma especial não regular e não for contrário a esta.

---

[168] GUARDIAN, *The- Londoners give up eldest children in public Wi-Fi security horror show*. [Em linha]. [2014]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>.

[169] COSTA, Francisco Bruto da e BRAVO, Rogério – ***Spam e Mail-Bomb* subsídios para uma perspetiva penal**. Lisboa: Quid Juris, 2005, p.22.

[170] Art.º 217º do Código Civil português.

4.2 Manifestação de Vontade Livre

Neste contexto, faz-se necessário analisar o Consentimento livre[171], ou seja, diante das ofertas aliciantes que são direcionadas a cada pessoa ao aceder à internet, onde o *Big Data* faz o seu papel com grande louvor, será que o Consentimento pode ser considerado livre? Observa-se que o *Big Data* se vale de meios específicos para fazer previsões de preferências das pessoas das mais ocultas imagináveis, como já foi anteriormente explanado, sendo certo que age no psicológico das pessoas.

Está implícito que, o facto de ser de livre vontade, nos casos de execução de um contrato subordinado ao tratamento de dados pessoais que não sejam necessários para a execução desse mesmo contrato pode-se afirmar que, nestes casos, o Consentimento não é válido.

O Consentimento é considerado livre quando é o resultado de uma decisão voluntária, segundo os Princípios Gerais de Direito Civil e do Direito à Proteção de Dados Pessoais, sem que exista qualquer tipo de coação[172], que pode ser de caráter:

-Psicológico;

-Social e

-Financeiro.

Sendo o resultado do não-consentimento impeditivo de privar e apresentar consequências[173] que possam comprometer a liberdade de escolha da pessoa. Dito isto, no caso dos dados recolhidos via *Big Data*, que possuem o poder de influenciar os negócios jurídicos no ciberespaço e fora dele, cabe aos aplicadores do direito analisar a cada caso a questão da validade do Consentimento.

Ainda no universo de proximidade da coação[174], é importante ressaltar que no Direito Inglês (*Common Law*), existem duas modalidades de *undue influence*:

- *Presumed undue influence* e

- *Actual undue influence*

[171] Art.º 7.º, n. º4 do RGPD.
[172] Art.º 255º do Código Civil dispõe sobre coação moral.
[173] Considerando 42 do RGPD.
[174] CORDEIRO, António Barreto Menezes - **Direito inglês dos contratos I - Formação, Conteúdos, Vícios**. AAFDL, Lisboa, 2017.

Presumed undue influence é considerada nos casos em que uma pessoa possuindo uma posição elevada em relação à outra, faz uso dessa posição, e o Consentimento nestes casos tem a possibilidade de ser viciado, tornando-se ineficaz. O facto de existir de uma desigualdade, onde a parte mais frágil é quem deve tomar a decisão de conceder ou não à outra parte mais forte, faz com que não tenha opção de escolha livre e independente. A influência presumida é como se fosse uma influência originária. Como exemplo a relação entre pessoas casadas, pais e filhos e etc.

Já nos casos de *Actual undue influence*, diferente da precedente, são os casos em que se apresenta qualquer relação entre duas partes que não seja uma relação presumida de posições diferentes e assim decorrente de factos posteriores como um contrato de trabalho, advogados e seus clientes, médicos e seus pacientes e etc., por exemplo. São nos casos em que aparece uma das partes numa posição elevada em relação a outra, o que pode viciar o Consentimento[175].

Desta forma, muito seria válido se a figura do *Common Law* do Direito Inglês, fosse adotada na vida prática dos tribunais portugueses, que possuiriam mais um meio na tutela de pessoas referente aos dados pessoais.

4.2.1 Desequilíbrio Manifesto

O considerando 43 do RGPD traz a figura do desequilíbrio manifesto, no que segue:

"A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo

[175] CORDEIRO, António Barreto Menezes - O consentimento do titular dos dados no RGPD, p. 11. [Em linha]. [2018]. [Consult. 20 fev. 2019]. Disponível em WWW:<URL:https://blook.pt/publications/publication/e772e2d8f7b4/>.

a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução."

Assim, deverá ser rogado a figura do considerando supramencionado sempre que existir a desproporcionalidade entre as partes e a figura do Consentimento, sendo certo que o mesmo não pode ser considerado válido nestes moldes.

O desequilíbrio manifesto não é de todo esclarecido seja por lei ou por jurisprudência. Até ser produzida jurisprudência sobre o assunto, pode-se considerar como pessoas desta categoria:

- Consumidores,

- Investidores,

- Trabalhadores,

- Doentes e

- Contribuintes ou cidadãos quando das relações com os Estados. (A. Barreto Menezes, 2018).

Cada situação deverá ser analisada individualmente, sendo a desproporcionalidade das partes e o prejuízo que possa resultar para a parte mais fraca, que coloca em situação de alerta a veracidade do Consentimento em causa.

4.3 Manifestação de Vontade Específica

O Consentimento específico existe nos casos de tratamento de dados pessoais com fins determinados[176] e concretos, devendo cumprir os fins que foram aceites pelos titulares e não mais que isso, sendo que somente poderá ter o *status* de específico se for informada esta ligação, que é sedimentada pelo GT29[177].

Foi decidido pelo TJUE, através do Acórdão *Deutsche Telekom AG v Bundesrepublik Deutschland*, decisão que vai de encontro com o que está especificado no RGPD, não ser necessário renovar o Consentimento quando o segundo pedido para um segundo

[176] Grupo de Trabalho do Artigo 29.º - Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679 (17/PT WP259 rev.01). [Em linha]. [2017]. [Consult. 21 jan. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf>.
[177] *Idem*, p 11.

tratamento, tiver as finalidades similares da original já concedida. Ou seja, os titulares uma vez autorizando o tratamento dos dados pessoais numa situação, tal servirá para uma segunda situação se esta for igual à primeira[178]. Decisões deste género deverão ser vistas com muita cautela, uma vez que os titulares podem já não desejar que o tratamento dos dados pessoais seja realizado. Mesmo sabendo da possibilidade do cancelamento, podem ter a intenção de autorizar o tratamento para somente um ato e não para vários outros, a não ser que seja exposto tal possibilidade no ato do primeiro Consentimento.

4.4 O Consentimento e a Prova

O RT assume todos os deveres da legalização do tratamento de dados pessoais, devendo ser específico e conservar todos os registos das atividades resultante do tratamento.

Segundo o Considerando 82: "A fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento."

Cabe ao RT fazer prova da existência de que houve o tratamento de dados com anuência dos titulares dos dados pessoais. De acordo com o Art.º 7.º, n.º 1 do RGPD, é responsabilidade do RT a demostração do Consentimento válido. Também ganha reforço das responsabilidades o disposto no Art.º 5.º, n.º 2 da mesma legislação.

Dado o exposto, pode-se chegar a conclusão que não existe nenhum tipo de Consentimento de carácter obrigatório, sendo que as obrigações oriundas de lei não carecem de ser submetidas a Consentimento. Deve ser afastado a possibilidade de coação no momento da celebração de contrato.

[178] Acórdão do processo n.º C-543/09 TJUE (*Deutsche Telekom AG v Bundesrepublik Deutschland*), p. 65.

4.5 A Revogação do Consentimento

No plano da revogação[179], está explícito no n.º 3, do art.º 7º do RGPD, a possibilidade de os titulares dos dados pessoais exercerem o direito de retirar o seu Consentimento a qualquer momento e que seja de forma tão fácil como aquela em que foi dado.

Assim, a revogação do Consentimento que foi dado deve ser acautelada pelo direito da proteção de dados pessoais e direito civil, no tocante aos interesses do RT, que é parte contratual.

Pode-se afirmar que, para exercer o direito à revogação se deve observar o Art.º 334.º do CC, mesmos nos casos em que não exista uma relação contratual, e o Art.º 762º. n. 2 do CC, se for cabível (A. Barreto Menezes, 2018). Nunca descurando a existência do princípio da boa-fé.

4.6 Responsabilidade Civil

As pessoas, com o passar do tempo devido ao desenvolvimento tecnológico, possuem a necessidade de serem mais tuteladas no que toca aos seus dados pessoais, levando em consideração as formas hodiernas de recolha e armazenamento de informações por parte de terceiros e pelo poder público[180].

O RGPD reforça a questão das responsabilidades e não traz novidades específicas sobre a matéria. Como necessidade de dar cumprimento ao RGPD, ficam o RT e o subcontratante (se existir) responsáveis por suportar o pagamento de indemnizações que decorram de danos na esfera jurídica dos titulares de dados pessoais na decorrência de violações da norma em questão[181].

Segundo o Considerando 146, o RT e o subcontratante assumem a reparação de danos de eventuais vítimas de tratamento indevido de dados pessoais que venham a ferir o diploma, cabendo aos mesmos fazerem prova de que o facto que originou os danos não era de sua responsabilidade, sendo desta forma exonerados.

---

[179] Sobre o Consentimento e a sua revogação nos termos do n.º 2, do art.º 81º do CC. "A revogação do consentimento deve dar lugar à imediata destruição dos dados e é lícita, embora possa fazer incorrer o titular na obrigação de indemnizar os danos causados pela revogação". VASCONCELOS, Pedro Pais de - **Proteção de Dados Pessoais e Direito à Privacidade- in Direito da Sociedade da Informação**. Coimbra: Coimbra Editora, 1999, p. 252.

[180] MIRANDA, Jorge e MEDEIROS, Rui de - **Constituição Portuguesa Anotada, tomo I**. Coimbra: Editora Coimbra, 2005, artigo 35º, p. 379-380.

[181] Art.º 82 do RGPD.

Em relação ao dano, deve-se considerar em sentido lato à luz da jurisprudência do Tribunal de Justiça, que faça valer o pensamento dos objetivos do RGPD. A responsabilidade poderá ser afastada se o RT ou o subcontratante provarem que não são responsáveis pelo evento que deu origem aos danos.

Todas as vezes que o RT e o subcontratante estiverem a trabalhar com dados em comum, poderá somente um responder pelo integral pagamento dos danos causados, sendo possível a repartição da indemnização conforme a participação nos casos em que os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros.

Qualquer responsável pelo tratamento ou subcontratante que tenha sido responsabilizado a uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento. Os sujeitos que estão relacionados no Art.º 82.º do RGPD são exclusivamente o RT e o subcontratante. Nos casos de os titulares entenderem de alguma forma estarem prejudicados por outras pessoas[182], deverão argumentar com o Art.º 483.º do CC[183], sendo tal a forma mais correta. O RGPD tem como regra a solidariedade obrigacional entre os corresponsáveis (para que seja considerado controlo conjunto e, portanto, para que possamos falar de co-controladores torna-se importante que exista efetiva partilha das finalidades e dos meios[184]) enquanto inverte o ónus da prova[185].

Levando em conta o que foi observado, nota-se que há mais facilidades para que o lesado se possa defender quanto ao uso indevido dos seus dados pessoais, possibilitando a este, responsabilizar diretamente o RT e o subcontratante. A existência da responsabilidade solidária também reforça essas facilidades.

---

[182] BARBOSA, Mafalda Miranda - *Data controllers e data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil. [Em linha]. [2018]. [Consult. 22 jan. 2019]. Disponível em WWW:<URL:https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5aaacd451ae6cf02516c4b66/1521143111492/2018-10.pdf>.

[183] Referente ao princípio geral – "1. Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação.2. Só existe obrigação de indemnizar independente de culpa nos casos especificados na lei."

[184] BARBOSA, Mafalda Miranda - *Data controllers e data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil**.** [Em linha]. [2018]. p. 18 [Consult. 23 jan. 2019]. Disponível em WWW:<URL:https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5aaacd451ae6cf02516c4b66/1521143111492/2018-10.pdf>.

[185] Art.º 82.º, n. º 3 do RGPD.

CAPÍTULO V – OS DIREITOS ELENCADOS NO REGULEMENTO GERAL DE PROTEÇÃO DE DADOS

Para além da Abordagem Baseada no Risco e a Abordagem de Autodefesa, os titulares dos dados necessitam utilizar todos os meios de defesa disponíveis.

É importante ter conhecimento dos direitos que constam no RGPD de forma a que, para além de poderem fiscalizar o uso pelas empresas dos seus dados pessoais, poderem exigir nos contratos a devida tutela cabível. Faz-se necessário ter o conhecimento dos direitos que orbitam nesta matéria.

5.1 Direito de Acesso do Titular dos Dados

O Direito de Acesso do Titular dos Dados[186] é um direito que permite obter informações sobre os dados que lhes digam respeito, nomeadamente se há tratamento, se há transmissão para outra entidade e ter acesso aos mesmos. Pode-se dizer que é um complemento a autodeterminação informacional.

O Tribunal Europeu dos Direitos do Homem (TEDH) já havia afirmado em alguns acórdãos que todas as pessoas possuem o direito de acesso a informações sobre os seus dados pessoais detidos ou utilizados por terceiros, sendo este direito o resultado do respeito à vida privada das pessoas[187]. "A autodeterminação informacional implica todas as possibilidades de um *facere*, de uma liberdade comunicacional sem nunca perder a sua marca d'água originária, ou seja, a defesa contra a intrusão indevida da esfera da personalidade do indivíduo" (PINHEIRO, 2015). Desta forma, existe uma forte relação do direito de acesso com a autodeterminação informacional, pois para que a pessoa possa fazer valer o direito supramencionado, deverá ter o domínio dos seus dados pessoais que estão a ser tratados. Para que possa determinar qual informação pessoal que autoriza o tratamento, o acesso aos dados é uma garantia pessoal. Também apresenta relação com os direitos de retificação e ao apagamento.

[186] Art.º 15.º do RGPD.

[187] TEDH, acórdão Godelli c. Itália de 25 de setembro de 2012, petição n.º 33783/09; TEDH, acórdão K.H. e outros c. Eslováquia de 28 de abril de 2009, petição n.º 32881/04; TEDH, acórdão Gaskin c. Reino Unido de 7 de julho de 1989, petição n.º 10454/83; TEDH, acórdão Odièvre c. França [GS] de 13 de fevereiro de 2003, petição n.º 42326/98 entre outros.

O RT é quem fornece resposta todas as questões solicitadas, informando sobre as finalidades, a categoria de dados a usar, os destinatários, o prazo de conservação dos dados, a possibilidade que os titulares dos dados têm para a retificação, apagamento ou limitação do tratamento dos dados, a possibilidade de poderem apresentar reclamação a uma autoridade de controlo, a origem dos dados quando os mesmos não forem recolhidos junto ao titular e a existência de decisões automatizadas e as suas consequências.

Quando não existe indicação das finalidades dos dados, não existe legitimidade para a sua recolha, nem tratamento dos mesmos. O direito de acesso possui um papel de caracter fiscalizador sobre a legitimidade dos atos a serem tratados segundo Pinheiro (2015, p. 945).

Prima facie, a informação elencada tende a ser gratuita e oferecida através de uma cópia dos dados pessoais que estão a ser tratados, mas nos casos de pedidos infundados ou excessivos poderá ser criado a obrigação de pagamento para o efeito.

5.2 O Direito de Retificação

O Direito de Retificação[188] é o direito que o titular possui de retificar os dados inexatos, tendo como objetivo a correção de informações inverídicas ou erróneas, desatualização ou dados incompletos, ainda que lhe sejam favoráveis. Não é um direito novo, uma vez que já se encontrava na Diretiva n.º 95/46/CE.

Em algumas situações o RT poderá sim recusar a realização da complementação de dados que venha a ser solicitado por algum titular, devido ter de seguir a legislação que define que os dados devem ser adequados, pertinentes e limitados, sendo apenas os necessários para os quais justifica o tratamento dos mesmos[189].

5.3 Direito ao Apagamento

O direito ao apagamento não é novo, uma vez que se trata de proteção da vida privada e intimidade das pessoas. Como forma exemplificativa pode-se citar:

[188] Art.º 16.º do RGPD.
[189] PINHEIRO, Alexandre Sousa [et al.] – **Comentários ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, p. 364.

-O caso *Lebach* – facto ocorrido com soldados alemães na cidade de Lebach, onde quatro soldados foram assassinados. Após o julgamento, três réus foram condenados. Sendo que dois receberam a prisão perpétua e o terceiro condenado a três anos de reclusão. Ao fim do cumprimento da pena, antes do mesmo deixar a penitenciária, tomou conhecimento que iria passar na televisão o caso ocorrido e além do fatídico ocorrido, ainda expor a intimidade dos reclusos. Em decorrência da exposição que o ex-recluso iria sofrer, ingressou com uma ação inibitória com a finalidade de impedir a exibição do programa. Ação chegou até o Tribunal Constitucional Alemão que decidiu que a proteção constitucional da personalidade teria preferência sobre o direito à informação segundo Ataíde (2018, p.3).

O direito ao apagamento[190] é abalizado no cenário hodierno, tendo em consideração todas as tecnologias e serviços disponíveis. Sendo considerado uma novidade do RGPD, também é conhecido como o "direito a ser esquecido". Os titulares dos dados possuem o direito de solicitar ao RT o apagamento dos dados que lhes digam respeito, respeitando os limites legais.

O direito ao apagamento referido, é estendido não só para os dados proibidos[191] (como nos casos que deixam de ser necessários ou são ilícitos), ou que se tenham tornado proibidos[192], (quando exista a retirada do Consentimento para o tratamento), como em todos as situações lícitas de tratamento de dados, inclusive o tratamento de dados que seja permitido.

O exercício do direito ao apagamento não pode afetar, designadamente:

- O cumprimento de obrigações legais;

- Razões de interesse público na área da saúde pública;

- O tratamento para fins de arquivo público, investigação científica e fins estatísticos e

- O exercício de direitos em processos judiciais.

Em virtude do que foi mencionado, o direito ao apagamento pode ser considerado como uma etapa do direito de oposição. O direito ao apagamento deve ser exercido em primeiro lugar, para que os titulares dos dados não deixem dúvidas sobre a insatisfação pelo uso dos seus dados.

[190] Art.º 17.º do RGPD.
[191] Art.º 17.º, n.º 1, alíneas a) e d) do RGPD.
[192] Art.º 17.º, n.º 1, alínea b) do RGPD.

Desta forma, todas as precauções deverão ser comprovadas, para manifestar sua insatisfação e consequentemente o apagamento, cabendo ao RT fixar prazos certos para a realização do feito[193].

5.4 Direito à Limitação do Tratamento

Direito à limitação do tratamento[194] é previsto no RGPD com a finalidade dos titulares dos dados poderem limitar o tratamento dos dados nas seguintes situações:

- Contestar a exatidão dos dados;

- Quando se tratar de tratamento ilícito;

- Quando deixar de existir o motivo para que os dados foram coletados, não sendo mais necessários para a finalidade original, mas ainda não puderam ser apagados por razões jurídicas ou

- Enquanto os titulares dos dados aguardam a decisão sobre a objeção do titular ao tratamento.

Posto isto, existe a possibilidade de solicitar a limitação do tratamento dos dados para garantir que os mesmos não sejam utilizados para fins diversos e indesejados.

Como exemplo, supondo que exista um banco novo no mercado interno que apresenta ofertas no crédito imobiliário com melhores condições que as existentes no mercado. Uma pessoa resolve mudar o seu banco para aproveitar as oportunidades do novo banco, e para isso, solicita ao banco antigo que encerre todas as contas e que apague todos os seus dados pessoais. Porém, existe uma legislação própria dos bancos que impede essa solicitação do cliente, sendo obrigados a manter os registos por um período de 10 anos. Sendo assim, o cliente solicita a limitação do tratamento, impedindo o uso dos dados pessoais para outros fins, especificando o uso somente para cumprir, no caso do exemplo, disposição legal.

[193] Considerando 39 do RGPD.
[194] Art.º 18.º e considerando 73 do RGPD.

5.5 Direito de Portabilidade dos Dados

O direito de portabilidade[195] é uma das novidades do RGPD, não estando presente na legislação anterior de proteção de dados. Este direito está nitidamente ligado ao direito de Acesso apesar de possuir aspetos diversos.

Consiste na opção dos titulares dos dados de solicitar ao RT a transferência dos seus dados para outro responsável, em formato estruturado, de uso corrente e de leitura automática, sendo em formato de uso comum na transferência dos dados pessoais para o próprio titular.

O Art.º 20º do RGPD faz referência ao conteúdo do considerando 68, que apresenta uma justificação da matéria. A portabilidade tem como finalidade reforçar o controlo dos dados pessoais, sempre que forem de tratamento automatizado, consentido pelo titular ou derivado de tratamento que foi necessário à utilização dos dados pessoais para a execução do contrato, e também oferecer aos titulares um papel ativo no ecossistema de dados.

A matéria supramencionada tem claro objetivo de favorecer aos titulares dos dados pessoais o controlo sobre os mesmos. Quando o tratamento se basear no Consentimento e for realizado por meios automatizados, os titulares podem solicitar ao RT a entrega dos seus dados pessoais a outro RT, permitindo a verdadeira liberdade de escolha dos titulares dos dados em relação a quem permite o tratamento dos mesmos.

Esta possibilidade vai facilitar a mudança de prestadores de serviços e proporcionará a criação de novos serviços e novas oportunidades de ofertas de produtos. Os dados pessoais que foram fornecidos pelos titulares de forma ativa e consciente e também os dados pessoais que são obtidos pelo extrato das atividades dos mesmos, são abrangidos pelo Direito à Portabilidade[196].

O Art.º 20.º do RGPD apresenta como características principais:

- O direito de receber os dados pessoais que estejam num formato estruturado, de uso corrente e de leitura automática;

- O direito de transmitir os dados pessoais de um RT para outro RT e

- Um controlo maior dos dados pessoais.

---

[195] Art.º 20.º do Regulamento.

[196] Grupo de Trabalho do Artigo 29.º - Orientações Sobre o Direito à Portabilidade dos Dados (16/PT WP 242 rev.01). [Em linha]. [2017]. [Consult. 5 dez. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf>.

Como limite do direito à portabilidade, encontra-se no Art.º 20.º, n.º 4 do RGPD que o referido direito não pode prejudicar direitos e liberdades de terceiros. O titular dos dados é, desta forma, chamado a decidir ou solicitar sobre questões em que possam envolver os seus dados pessoais, o que antes era matéria de domínio das empresas, que resolviam todo o tipo de destino dos dados pessoais armazenados. O RT dos dados é, desta forma, responsabilizado frente aos titulares dos dados, nos casos que o tratamento não seja adequado às finalidades originais.

Se não existisse o direito de portabilidade, o titular dos dados ficaria numa situação de aprisionamento com a empresa atual (DUARTE, 2018). Como exemplo: se o titular dos dados ao decidir a mudança de prestador de serviços de e-mail, tivesse de perder todas as informações contidas no mesmo, não seria adequado tomar tal decisão. Pode-se considerar que o titular se submeteria como refém de alguns contratos, principalmente de carácter profissional. A mesma situação se pode alegar nos contratos bancários, se ao trocar de instituição bancária os titulares dos dados perdessem todo o histórico da relação, que muitas vezes são de muitos anos, poderia não trocar de banco uma vez que no novo banco poderia ter dificuldades para algumas operações financeiras pela inexistência de histórico[197].

O direito em questão também apresenta riscos, os mesmos que podem resultar em perigos de abusos no momento da realização de contratos. Como exemplo, o contrato de um seguro de saúde em que o operador pode colocar como requisito para a realização contratual, que os titulares dos dados pessoais façam valer o seu direito a portabilidade, levando desta maneira todos os seus dados de saúde ao mesmo, condicionando a não realização contratual caso o titular dos dados não ceda às exigências.

Quando aparece como condição obrigatória para a realização contratual o direito de portabilidade dos dados, tal é sem dúvida um abuso de direito que deverá ser analisado e responsabilizada a sua prática[198]. Os abusos deverão ser combatidos para que não se use a legislação com efeitos desfavoráveis às pessoas (DUARTE, 2018).

[197] DUARTE, Diogo Pereira - A Portabilidade dos dados. I Jornadas de Proteção de Dados e Empresas. Faculdade de Direito da Universidade de Lisboa – CIDP. [Em linha]. [2018]. [Consult. 12 jan. 2018]. Disponível em WWW:<URL:https://youtu.be/zoUTP8eeuco>.

[198] DUARTE, Diogo Pereira - A Portabilidade dos dados. I Jornadas de Proteção de Dados e Empresas. Faculdade de Direito da Universidade de Lisboa – CIDP. [Em linha]. [2018]. [Consult. 12 jan. 2018]. Disponível em WWW:<URL:https://youtu.be/zoUTP8eeuco>.

5.6 Direito de Oposição ao Tratamento

O direito de se opor[199] a qualquer tratamento é inerente aos titulares dos dados. Os motivos alegados devem ter relação com a situação particular[200] de cada pessoa, sendo que em certas situações a oposição é sempre admitida, como nos casos de comercialização de venda direta.

Nos casos de tratamento de dados que é realizado no âmbito de necessidade ao exercício de funções de interesse público ou nos casos de exercício de autoridade pública ou por motivo de interesse público do RT, os titulares continuam a ter direito ao exercício do referido direito, sendo de responsabilidade do RT a comprovação de que o seu interesse legítimo sobrepõe aos interesses ou direitos e liberdades fundamentais dos titulares.[201]

5.7 Direito de Não Ficar Sujeito a Decisões de Tratamento Automatizado

As decisões que sejam tomadas com base em tratamento automatizado[202] de forma exclusiva, permitem aos titulares dos dados exercer o direito de não sujeição, principalmente quando possam produzir efeitos na esfera jurídica ou de outra forma similar. As exceções são:

- Se for necessário para a elaboração ou a execução de contrato entre o titular dos dados e o RT;

- For autorizado por lei, salvaguardando os direitos e liberdades dos titulares e

- For baseado no Consentimento explícito do titular dos dados.

[199] Art.º 21.º do RGPD.
[200] Este direito encontra limitações no RGPD quando o tratamento de dados pessoais tenha como base o artigo 6.º, n.º 1, alínea e) ou F) ou no artigo 6.º, n.º 4 com inclusão de perfis com base nessa disposição.
[201] Considerando 69 do RGPD.
[202] Art.º 22.º do RGPD.

CAPÍTULO VI – OS DADOS PESSOAIS E AS RELAÇÕES JURÍDICAS

6.1 As Relações Jurídicas à Luz do RGPD

O atual desenvolvimento tecnológico está a resultar numa nova sociedade, sem fonteiras e sem homogeneidade cultural. Desta forma, o mundo digital ganha grandes proporções, sendo uma disrupção às relações jurídicas tradicionais. Atualmente, as fronteiras e as distâncias não são óbices à celebração de negócios jurídicos sejam eletrónicos ou não

As relações jurídicas realizadas através dos meios eletrónicos não são uma figura nova no ordenamento jurídico, porém, com o RGPD ganham uma nova forma de protagonismo pragmático

6.2 Contratos que Oferecem Serviço Digitais que Tenham como Contrapartida Dados Pessoais

O RGPD entra num cenário em que a definição de perfis é um aliado para a tomada de decisões pelo que a definição dos mesmos e as decisões automatizadas são utilizadas em muitas áreas. A atividade bancária, financeira, a saúde, a fiscalidade, os seguros, o marketing e a publicidade são exemplos onde se usa a definição de perfis para auxiliar as tomadas de decisões[203].

Existem contratos **(**nos casos de contratos informáticos, entende-se que são aqueles que que possuem como objeto bens corpóreos e incorpóreos que visam a possibilidade do tratamento automatizado de informação, a colocação de conteúdo em linha e a prestação de serviços) [204] que oferecem serviços digitais que têm como contrapartida dados pessoais. Estes serviços são oferecidos geralmente de forma gratuita[205] permitindo por exemplo a interação em redes sociais, entre outros, como é o caso do Facebook. As informações surgem como um bem negociável e são entendidas como bens económicos (KLOTZ, 2000).

As autorizações para o tratamento dos dados pessoais deste tipo de contrato, na grande maioria, possuem nas cláusulas o Consentimento que ultrapassa as necessidades para a realização do serviço.

---

[203] Grupo de Trabalho do Artigo 29.º - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 (WP251rev.01). [Em linha]. [2018]. [Consult. 15 dez. 2018]. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/ WP251rev.01_pt.pdf

[204] VICENTE, Dário Moura – **Problemática Internacional da Sociedade da Informação**. Coimbra: Almedina, 2005, p. 246.

[205] HARTZOG, W.; SELINGER, E.- *Big data in small hands.* [Em linha]. [2013]. [Consult. 16 jan. 2019]. Disponível em WWW:<URL:https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-in-small-hands/>.

A partir do Consentimento (que deve ser uma manifestação de vontade, livre, específica, informada e explícita), as organizações passam a conhecer todas as preferências das pessoas, oferecendo produtos que se adequem a elas, entre outras tantas possibilidades (HARTZOG e SELINGER, 2013).

O utilizador do serviço, que é visto como gratuito, consente a alienação dos dados para terceiros. Tal Consentimento, que é realizado pelo titular dos dados, não sendo instrumental para a efetivação do serviço, é o que se pode chamar de contraprestação. Nota-se, portanto, que houve o Consentimento de acordo com o RGPD para a utilização dos dados pessoais, em contrapartida dos serviços prestados pela operadora, sem valor pecuniário a ser pago.

Os serviços gratuitos que são oferecidos possuem uma estratégia muito interessante. Com as empresas que oferecem serviços na internet, não ocorrendo nenhum pagamento pecuniário, a relação estabelecida não pode ser de consumo. Desta forma, o "produto" é a pessoa e os seus dados pessoais, sendo considerada o produto-final da relação contratual (HARTZOG e SELINGER, 2013).

No mesmo contrato supramencionado, uma das questões de importância proeminente é saber o que toca à verdade dos factos, uma vez que os dados de origem *Big Data* podem não serem verdadeiros, e na esfera contratual é facto relevante para prosseguir com a relação sinalagmática. Nas relações contratuais, quando há informações falsas, alega-se exceção de não cumprimento ou resolução contratual mediante dados falsos, ficando garantido ao prestador de serviços a suspensão do contrato até que tenha sido sanado o vício, com a devida retificação dos dados. Outra alternativa seria a resolução do contrato[206] alegada pelo prestador de serviço.

De acordo com o RGPD, os titulares dos dados pessoais possuem sempre a competência de revogar o Consentimento a qualquer momento. Porém, não constam no mesmo diploma legal as situações em que o Consentimento é a contraprestação contratual, sendo esse tipo o mais habitual. Pelo exposto, não se pode aplicar o princípio do *Pacta sunt servanda* nestes casos.

Quando uma das partes resolve fazer valer o seu direito de revogar o Consentimento, sendo tal medida oriunda do ordenamento jurídico, sendo um exercício lícito, é considerada uma perturbação contratual em que não se pode imputar a nenhuma das partes nenhum juízo de censura.

Quando está em tela contrato de personalidade[207], em que estão incluídos os contratos de dados pessoais, segundo o código civil português, poderá a qualquer momento o titular do direito de personalidade denunciar o contrato, devendo, porém, indemnizar a outra parte pelos prejuízos. O RGPD deve-se coadunar com o direito interno, uma vez que teve preocupação robusta na tutela do

[206] Art.º 801 a 808 do Código Civil Português.
[207] Art.º 81.º n.º 2 do Código Civil Português.

direito à autodeterminação informacional. Porém, no direito interno, o cancelamento de um contrato, nesta hipótese, resultará na obrigatoriedade de indemnização.

Os dados pessoais adquiridos em contraprestação de serviços digitais, que tenham como finalidade a alienação dos mesmos a terceiros, despertam interesses das instituições, que se mostram dispostas a pagar por eles, devido a relevância do histórico que os mesmos trazem para as empresas. A venda desses dados a terceiros proporciona elevados lucros, existindo empresas que se dedicam exclusivamente ao mercado de compra e venda de dados pessoais, os chamados *Data broker*[208].

A alienação de dados pessoais, em especial os derivados de *Big Data*, que são decorrentes de contratos realizados entre os titulares dos dados e um fornecedor de serviço e que foram submetidos aos titulares através do Consentimento (regulado pelo RGPD) podem ser alienados para terceiros, e este aliena para um quarto e este aliena para um quinto e assim sucessivamente. A alienação citada é referente à faculdade de dispor desses dados em que o primeiro está habilitado legalmente, não é referente ao direito de autodeterminação informacional que é personalíssimo (BASTOS, 2018).

O RGPD não faz referência a este tipo de alienação muito comum atualmente. É importante verificar que nesta cadeia sucessiva de venda de dados pessoais não existam incompatibilidades de transmissão. O facto de várias empresas possuírem os dados do mesmo titular, com todas estando habilitadas para os usarem simultaneamente, não é uma transmissão como acontece com um bem (BASTOS, 2018).

A partilha de dados que se observa é a distribuição que pode ser gratuita, pública ou privada, de dados através da internet. Para alguns autores, a partilha não seria a palavra adequada para a situação, devido ao significado da palavra que significa repartir ou dividir em partes. O que acontece são reproduções automáticas de ficheiro digital, com o utilizador e os detentores a ficarem sempre na posse do conteúdo (LIEBOWITZ, 2004).

Abordando uma outra questão da mesma relação contratual, pode-se ter uma empresa que possui um s*oftware* que analisa preferências de clientes, sendo abastecido por *Big Data*, que por sua vez utiliza os algoritmos de *Machine Learning*. Como já foi exposto, é necessário um grande volume e variedade de dados disponíveis para abastecer o *software* de Inteligência Artificial, para que possa aprender a partir de informações novas. Somente com o passar do tempo e esse abastecimento de dados se chegará ao desiderato proposto sobre a eficácia do sistema que é a aprendizagem das máquinas de forma independente (SHALEV e BEN, 2014).

---

[208] Têm como finalidade a venda de informações pessoais dos utilizadores para empresas, com informações completas de atividades que são compiladas no histórico de navegação na internet. PEIXOTO, João Paulo – Vigilância Eletrónica: uma realidade desconhecida para a generalidade dos portugueses. [Em linha]. [2014]. [Consult. 20 jan. 2019]. Disponível em WWW:<URL:https://comum.rcaap.pt/bitstream/10400.26/9217/1/Vigilancia.Electronica..pdf>.

Os dados que uma empresa pretende comprar de outra especializada em venda de dados pessoais, podem não corresponder com a veracidade dos mesmos, pois, nem sempre serão fornecidos dados verdadeiros, como já foi referido sobre os dados derivados de *Big Data*. Na questão da alienação dos dados pessoais entre as empresas era suposto os dados serem verdadeiros, para que a relação sinalagmática seja juridicamente correta.

Dado o exposto, os direitos elencados no RGPD de revogação do Consentimento e o direito ao apagamento dos dados (direito a ser esquecido) pode ser exercido somente entre o titular dos dados pessoais e a primeira empresa, até porque os titulares não fazem ideia de quantas empresas alienaram os dados e foram habilitadas a tratar dos mesmos. Não está previsto algum tipo de dever de comunicação destes factos no RGPD, como solução para este problema hodierno.

Assim como ocorreram as habilitações em cascata para tratamentos dos dados, a revogação deverá ser da mesma forma, revogando-as a todos.

Posto isto, deverá existir um controlo minucioso no que toca as alienações de dados pessoais, quando autorizados pelos titulares, entre empresas, para que a revogação do Consentimento prevista no RGPD seja eficaz. Caso, aconteça a revogação do Consentimento ou a solicitação para o apagamento dos dados, a partir deste momento o tratamento dos mesmos é proibido e ilícito. As empresas posteriores à primeira se não foram informadas, têm a opção de se valer do Art.º 16.º do Código Penal alegando a exclusão do dolo, uma vez que agiram de boa-fé. Cabe ressaltar que a forma de tornar o RGPD eficaz nessa matéria, seria a obrigação da comunicação da primeira empresa para com as demais (BASTOS, 2018).

6.3 Informações Recolhidas *online*

Tentando dar resposta para a questão da presente dissertação, cabe mencionar que os negócios jurídicos realizados entre as pessoas e as empresas, possuem como base tradicional as informações que foram oferecidas pelos clientes, sendo as mesmas de conhecimento e controlo deles. Fica o cliente, sendo a fonte das informações perante às empresas, como que se fosse um colaborador para a realização do acordo, sendo as informações filtradas, selecionadas e analisadas pelo mesmo.

Não se reconhece nenhum óbice na questão da recolha de dados via internet, quando tal recolha seja baseada numa adaptação dos meios clássicos de recolha de dados pessoais, para os meios modernos (LEAL, 2017). Como exemplo, a recolha de dados dos titulares através de email endereçado para a própria empresa, *apps* disponíveis, formulários, pesquisas ou outros meios quaisquer que estejam disponíveis na plataforma da empresa. Tal recolha via internet é fruto da relação sinalagmática estabelecida entre a empresa e o cliente, onde à luz do RGPD exista tal relação contratual, e desta

forma, seja estabelecido que à empresa é dado o Consentimento para tratar dos dados pessoais (Art.º 4.º, n.º11), realizar o tratamento dos dados pessoais (Art.º 4, º, n.º 2), que possui o RT (Art.º 4.º, n.º 7) todos do RGPD), sendo desta forma lícita a recolha de dados *online* sempre que for utilizada a plataforma da empresa como meio de angariação dos mesmos.

Porém, em tempo de *Big Data*, as empresas procuram clientes mais confiáveis, sendo assim, recorrem ao uso de tal tecnologia. A recolha de dados pessoais nesta hipótese é diferente da que foi relacionada anteriormente, sendo neste caso baseada no uso das ferramentas tecnológicas com angariação de dados em todas as plataformas a que as pessoas acedam e não somente na plataforma da empresa contratante. Assim, todo o tipo de acesso que uma pessoa realize no telemóvel, nos computadores, nos dispositivos ligados em rede, etc., resulta na criação de dados que são monitorizados, pois, quanto mais dados gerados e recolhidos, melhor é o desenvolvimento de *machine learning*, e consequentemente um perfil mais detalhado dos utilizadores. A tutela das pessoas deve ser constantemente analisada, pois, a evolução tecnológica é muito acelerada, como exemplo: hoje os telemóveis possuem a capacidade de rastrear os seus usuários em todos os lugares. Em virtude do cenário atual e com o intuito de resguardar, respeitar, direitos e liberdades fundamentais, o RGPD regula em alguns artigos o uso e o tratamento dos dados em larga escala (*Big Data*) que permitem o acesso aos dados pessoais que foram consentidos pelos titulares, e também dispõe outras formas de Consentimentos, com o intuito de restringir o acesso aos referidos dados na medida do possível, ficando certo que somente os operadores que forem autorizados possuírem permissão para utilização dos mesmos. Com a finalidade de alcançar a realização de um espaço de liberdade, segurança e justiça para todos[209].

A base de dados que as empresas possuem são vastas, além de possibilitar a previsão de preferências futuras dos seus clientes atuais, utilizam as informações como referência para a angariação de futuros clientes[210].

Desde a alvorada da sociedade humana, a boa-fé é a base para as relações entre as pessoas. Com a evolução do direito e da tecnologia, a índole ainda é a alma das relações contratuais. Dito isto, as informações que são oferecidas de forma clássica pelos clientes e as informações que são coletadas na internet, devem ser de conhecimento de ambas as partes qual quer que seja o tipo da relação, seja no estágio do pré-contrato como no do contrato. Nas relações entre as pessoas e no direito, encontra-se muito sedimentada a ideia de boa-fé. Esta deve ser considerada extensiva a todos os domínios em que exista algum tipo de relação, de vinculação entre duas ou mais pessoas (VARELA, 2017).

[209] Considerando 2 do RGPD.

[210] LEAL, Ana Alves - *Big data* e proteção de dados pessoais – desafios à luz do Regulamento Geral de Proteção de Dados. **Revista Vida Judiciária**. Maio/junho 2018.

As informações que são recolhidas no ambiente virtual e que não tenham como fonte as plataformas das empresas que possuem relação com os clientes, isto é, sejam oriundas de outras plataformas onde os clientes "naveguem" e que contribuem para a formação de opiniões sobre as pessoas, de forma positiva ou negativa, não podem ser utilizadas por nenhuma prestadora de serviços. Além de tudo, o facto de as informações provenientes de *Big Data* poderem ser falsas deverá ser levada em consideração. Em contrapartida se forem verdadeiras, as pessoas ficam subjugadas às empresas detentoras das informações e nessa hipótese todas as preferências e tendências das mesmas ficam expostas.

O extrato de uma análise verdadeira pode levar a situações discriminatórias quando da realização contratual, sendo utilizadas informações, recolhidas *online*, que são desconhecidas pelos titulares dos dados. Como já foi referido, a recolha de dados via internet é diferente da situação descrita no caso em que exista uma relação contratual.

Quando uma pessoa para aceder a uma dada plataforma faz uso do nome de utilizador e palavra-passe de outra empresa, esses dados que serão gerados na plataforma da segunda empresa sofrerão uma simbiose entre ambas empresas. Isto posto, a primeira empresa terá acesso a todos os dados gerados pela segunda plataforma, que não tem nenhuma relação com o tipo de negócio e ou plataforma desta. Como exemplo, para a pessoa entrar na plataforma *Blook*-Portugal é dado a alternativamente ao utilizador a opção de fazer login com a Google +, Facebook ou realizar o registo na plataforma. Assim ao utilizar a conta de utilizador noutras plataformas, permite uma combinação de dados[211]. Tal situação como é entendida pelo GT29, não parece ser válida, devido ferir os princípios norteadores do RGPD, uma vez que não se pode dar um Consentimento genérico para o tratamento de dados pessoais, para além do tempo de armazenamento dos mesmos que deverá ser limitado às finalidades.

Sempre que o tratamento de dados seja permitido à luz do RGPD, e como os dados que circulam pela internet são cada dia mais volumosos devido as funcionalidades dos *smartphones* e torna-se tentador que as empresas decidam pela utilização dos mesmos.

Como já foi mencionado anteriormente, a tecnologia evolui certamente de forma ágil, e não passará muito tempo, os *smartphones* serão ultrapassados por dispositivos ainda menores e mais portáteis[212], mais precisamente colados ou mesmo inseridos no corpo humano, como *chips*, capazes

[211] Segundo entendimento do GT29. Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e subcontratante» (WP169) p.77 [Em linha]. [2010]. p.77. [Consult. 1 dez. 2018]. Disponível em WWW:<URL:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>.

[212] Nota-se que existe uma inclinação na miniaturização dos componentes informáticos, a cada ano são lançados dispositivos ainda menores dos que já existem e que entusiasmam as gerações atuais.

de transmitir toda a informação biométrica da pessoa que o utiliza, entre outras informações, o que começa a ser referido como *smartpeople* segundo Carvalho (2018, p. 45).

A importância das informações disponibilizadas na internet tem fundamento, uma vez que entre outras hipóteses já relacionadas anteriormente, o cruzamento da data de nascimento de uma pessoa com o tráfego geral gerado pela mesma nas páginas que consulta na web, pode emitir uma previsão de proposta em relação a, por exemplo, uma camisola do clube da pessoa, com estampado nas costas a idade ou mesmo data de nascimento dela (BOTÃO ALVES, 2014).

Desta forma, o *Big Data* constitui um verdadeiro desafio para o direito por permitir uma contratação de serviços automatizada, valendo-se do uso de preferências ocultas das pessoas, mas que por *Analytics* se pode descobrir e utilizar para benefício empresarial, à revelia de todos os envolvidos.

Pese embora esteja já muito difundido o uso do *Big Data* no *marketing* empresarial e consequentemente se estabelece uma relação sinalagmática, o alcance é muito maior do que se imagina. Como exemplo, o uso de *Big Data* na construção civil permite obter informação relevante, do tipo de construção que as pessoas mais gostam, qual é a melhor época para construir e vender, não apenas o que construir, mas onde construir, etc., sem qualquer espécie de inquérito formal As empresas de construção podem ainda, antes do fim da obra, instalar sensores embutidos nas instalações que possibilitam realizar o controlo de dadas finalidades, como o controlo da energia das áreas comuns dos prédios, dentre vários outras, o que de forma automatizada pode alertar para a realização de manutenções dos equipamentos e obtenção de padrões de utilização. Um bom exemplo que se pode citar, é o da Brown University[213], que para decidir o local adequado para a construção de uma nova instalação da Faculdade de Engenharia, recorreu ao uso de *Big Data.*

O Brasil já se mostra preocupado com a *Big Data* no setor público. Quando o Ministério do Planejamento decidiu colocar em consulta pública a Instrução Normativa número 4[214], que possui como finalidade principal regular a compra de bens e serviços de tecnologia da informação no Governo Federal. Entre outros temas, está relacionado expressamente como proibido a contratação pelos órgãos de soluções de armazenamento massivo de dados, tipo *Big Data* e *Analytcs*[215]. Porém,

---

AUGUSTO, João C. - *Intelligent Environments: a manifesto*. Vol. 3, n.º 12 [Em linha]. [2013]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://hcis-journal.springeropen.com/articles/10.1186/2192-1962-3-12>.

[213] Localizada na Providence, Rhode Island, EUA, fundada em 1764, a faculdade é a sétima mais antiga dos Estados Unidos. Brown é uma instituição independente e coeducacional da Ivy League.

[214] É uma Instrução Normativa que dispõe sobre: O Processo de contratação de Soluções de Tecnologia da Informação e Comunicação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - O Sistema de Administração dos Recursos de Informação e Informática do Poder Executivo Federal. Revisão da Instrução Normativa – Participa. [Em linha]. [2014]. [Consult. 26 jul. 2018]. Disponível em WWW:<URL:http://www.participa.br/revisao-da-instrucao-normativa-no-4-de-2014/instrucao-normativa-n-4>.

[215] Anexo 4 da Instrução Normativa número 4.

tal uso é permitido nos casos em que os estudos técnicos e preliminares conseguirem demostrar uma grande vantagem técnica. As relações entre empresas e as pessoas abrangem muitos temas ou quase todos os temas do direito, por essa razão serão expostas algumas situações em que é questionável a angariação de dados via *Big Data* para determinados fins, como as que seguem.

6.4 *Big Data* e os Contratos de Seguro Saúde

Quando se analisa as relações sinalagmáticas, no setor da saúde, do uso de dados pessoais sem Consentimento[216], é importante salientar que as consequências poderão ser de todo o tipo.

Na execução contratual que implica o tratamento dos dados pessoais de forma mais ampla, onde muitos deles são dados sensíveis, as pessoas oferecem todas as informações possíveis às empresas, que muitas vezes se valem do uso de *Big Data* para o efeito. A finalidade desta é a precaução contra possíveis incumprimentos ou onerosidades que o cliente possa causar. Quanto mais abrangente é a cobertura do seguro, mais detalhada é a informação armazenada (SIMITIS, 1987).

Os clientes normalmente almejam a realização contratual e para este fim autorizam o uso dos seus dados pessoais, sendo assim que o mesmo se coloca na situação pré-contratual. A questão a ser analisada é em relação à variação de preço do contrato do seguro de saúde, conforme a avaliação que é feita. Muitas vezes não está especificado no contrato e o cliente não é informado de que serão usados os meios tecnológicos para recolha de dados.

O Consentimento que é fornecido pelos titulares dos dados normalmente não está claramente relacionado no sentido de condicionar a realização do ato negocial com as informações recolhidas na internet. Nos casos em que não exista acordo estipulado entre as partes, o Consentimento deverá ser analisado em cada caso em concreto (LEAL, 2017).

Importante ressaltar que não há amparo legal específico para a recolha e manuseio de dados oriundos de *Big Data*, sendo regulada juntamente com os demais dados contidos no RGPD. O caso deverá inicialmente ser analisado conforme as regras clássicas do direito, a começar pelo Código Civil no Art.º 232.º: "(Âmbito do acordo de vontades) O contrato não fica concluído enquanto as partes não houverem acordado em todas as cláusulas sobre as quais qualquer delas tenha julgado necessário o acordo".

[216] Art.º 6. º, n. º 1, alíneas b) a f) do RGPD.

O que normalmente se observa é que a finalidade apresentada nos contratos *online* se limita no sentido de melhorar a satisfação dos clientes ou melhorar a experiência do utilizador, o que como é de fácil perceção, desta forma não está conforme o RGPD.

A observação de uma ponderação cuidada e prévia deverá ser o início de qualquer negócio jurídico, a culpa *in contrahendo* é um fator preponderante na boa-fé contratual. A culpa *in contrahendo* é um instituto da responsabilidade civil quando, no caso de nulidade do contrato, uma das partes que tenha ou devesse ter o conhecimento do óbice tem o dever de indemnizar a outra parte (ROCHA e CORDEIRO, 1984).

Dado o exposto, nos casos de existência de decisões automatizadas tal deve ser exposto de forma clara para a outra parte, cumprindo o esclarecimento da lógica subjacente, relacionado com os Art.º s 13.º, n.º 2, alínea f), art.º 14.º, n.º 2, alínea g) e art.º 15.º n.º 1, alínea h) do RGPD.

As pessoas atualmente produzem dados muito rapidamente e geram desta forma um grande conjunto de informações sobre si próprias. Desta forma, qualquer relação jurídica em que uma das partes possui acesso às referidas informações, deve comunicar a outra parte do uso aos recursos tecnológicos atuais. E deve submeter ao crivo da outra parte o Art.º 4.º, n.º 2 do RGPD. Os hábitos desenvolvidos pela sociedade quanto ao uso das tecnologias na rotina diária de organizações e indivíduos, está a transformar as pessoas em "geradores ambulantes de dados" (MCAFEE e BRYNJOLFSSON, 2012, p. 5).

Os exemplos são inúmeros, porém a mero título exemplificativo da recolha de dados no setor da saúde, que podem dar azo nos contratos de seguro de saúde, temos:

-Medidores de frequência cardíaca – que atualmente possuem uma maior precisão, podendo ser uma banda para usar na cabeça, auriculares, pulseira ou uma faixa peitoral. Utilizam um sensor (*IoT*) interligado com um equipamento com capacidade de computação (formato *smartphone* ou outro) da pessoa, que possua a capacidade de recolha, armazenamento e análise da situação cardíaca;

-Pedómetro – Dispositivo que tem a capacidade de contar o número de passos que a pessoa realiza por dia. Pode parecer um meio simples diante de tanta tecnologia existente, mas esse aparelho tem a capacidade de analisar o grau de sedentarismo da pessoa.

-Uso de ferramentas de buscas na internet.

-Cartão de cliente dos supermercados – faz monitorização do tipo de alimentação das pessoas, podendo concluir se a alimentação das mesmas é saudável. Por exemplo, os hipermercados Continente possuem um cartão de cliente, sendo este mesmo cartão usado para o plano de saúde Wells.

- Monitor de pressão sanguínea que realiza a comunicação com o telemóvel via *Bluetooth*[217].

Desta forma, as pessoas passaram a utilizar dispositivos portáteis para monitorização da saúde, produzindo um manancial de dados que têm também o potencial de permitir às instituições de saúde poderem oferecer serviços médicos mais personalizados. Também geram dados que na maioria das vezes estão armazenados na nuvem e que possuem potencialidade para serem usados como base no momento da contratação do seguro de saúde.

6.5 *Big Data* e as Relações Jurídicas entre os Setores Bancário e Financeiro

A revolução tecnológica não poderia deixar de ser diferente no que tange ao uso de *Big Data* nos setores Bancário e Financeiro, setores que desempenham um papel de relevo na economia dos países. O uso de *Big Data* por estas instituições possui como objetivo principal um melhor controlo, uma análise mais detalhada das relações jurídicas, prover estratégias de investimento para compra e venda de certos tipos de ativos, oferta de taxas de câmbio em tempo real em todo o mundo, o que pode facilitar a realização de negócios e liquidações globais, entre outros.
São setores mais sensíveis no que tange a administração de volume de dados pessoais produzidos pelos clientes a cada minuto, dentro de um contexto de mercado competitivo. Tal competição é amenizada quando se fala em proporcionar maior eficiência e vantagens frente aos concorrentes. Inicialmente a adoção de *Big Data* nestes setores não foi um fenómeno de imediata adaptação pelas instituições, devido as inibições organizacionais e culturais (NATH, 2018). Atualmente o cenário foi alterado, sendo um dos setores que mais investe em *Big Data Analytics* é o setor Financeiro (IDC Worldwide, 2016).

[217] *Bluetooth* é uma tecnologia de comunicação sem fio a partir de ondas de rádio, possibilita que computadores, *smartphones*, *tablets* e outros troquem dados entre si e se conectem a teclados, fones de ouvido, impressoras, caixas de som, computadores e outros. A ideia consiste em possibilitar que dispositivos se interliguem com agilidade e sem uso de cabos, bastando que um esteja na proximidade do outro. InfoWester - Tecnologia *Bluetooth*: o que é e como funciona? [Em linha]. [2018]. [Consult. 4 jan. 2019]. Disponível em WWW:<URL:https://www.infowester.com/bluetooth.php#definicao>.

A importância no setor ora mencionado é devido ao tratamento de dois fatores importantes para a sociedade, que são os dados pessoais e o capital, e onde a descoberta de padrões ocultos nos seus clientes e não clientes, podem resultar na melhoria da oferta de produtos financeiros (quando muitas vezes o próprio cliente ainda não sabe do que necessitará no futuro próximo), para além da possibilidade de adquirir novos clientes (LEAL, 2017).

É através do uso de *Big Data* que as instituições podem conseguir:

- Análise pormenorizada em gestão de risco;
- Aumentar a estabilidade da instituição;
- Descobrir as necessidades dos clientes;
- Reduzir de riscos nas operações realizadas pelos clientes e
- Fiscalizar as relações com os clientes (MAROUS, 2012).

Desta forma, a importância das tomadas de decisões neste setor, que muitas vezes são em tempo real, levam à maior utilidade no recurso ao uso das tecnologias em questão, sendo certo que segundo o RGPD a licitude[218] deverá ser nos moldes em que apresente pelo menos uma das situações:

- Se comprovadamente for dado o Consentimento para o tratamento;
-Se for necessário para a execução do contrato com o titular dos dados;
- Se for para o cumprimento de uma obrigação jurídica;
- Se for na defesa de interesses vitais dos titulares dos dados ou de outra pessoa singular;
- Se for no exercício de funções de interesse público ou exercício da autoridade pública e
- Se for necessário para efeito dos interesses legítimos[219] prosseguidos pelo RT ou por terceiros.

Não sendo esta dissertação um trabalho direcionado somente para uma visão em relação ao uso de *Big Data*, é incontestável reconhecer que, entre outras vantagens, o uso de *Big Data* oferece mais segurança aos clientes das instituições financeiras no que tange a segurança das operações realizadas, mas sobre tudo, a certeza de que se houver operações financeiras suspeitas, que não constam dos hábitos dos titulares, estas terão grande possibilidade de ser impedidas ou anuladas em tempo real.

A relação estabelecida entre os setores Bancário e Financeiro e as pessoas também está fortemente interligada com o tráfego de dados no ciberespaço, onde a utilização de *Big Data* é direcionada para:

---

[218] Art.º 6.º do RGPD.

[219] O interesse legítimo é de difícil conceituação, é considerado de complexidade elevada no que toca a definição do mesmo. Sendo um dos fundamentos de licitude de tratamento de dados, restando aos aplicadores do direito a tarefa de interpretar e fazer a adequação da norma. CORDEIRO, A. Barreto Menezes – O tratamento de dados pessoais fundado em interesses legítimos. **Revista de Direito e Tecnologia** [Em Linha]. Vol. 1 (2019). [Consult. 15 mai. de 2019]. Disponível em WWW:<URL:https://blook.pt/publications/publication/29c85b840a65/?fbclid=IwAR3oZ8IJPPnm2qAz_w20CAr1WhdkG4Tbv4jjSFNBTo8Bs4oL_wm7LUP0mA>.

- Uso no plano comercial;
- Uso decisório e
- Uso regulatório.

O plano comercial está dividido em:

- Angariação de novos clientes e
- Fidelização de clientes (LEAL, 2017).

A angariação de novos clientes é baseada na procura do ajuste da oferta de produtos e serviços com o perfil das pessoas, da forma mais adequada possível. E para que se alcance o êxito da relação, a coleta de dados de investigação é baseada em:

-Monitorização de comportamentos;
-Preferências e
-Análise de padrões de consumo.

O comportamento das pessoas sofre influência por vários setores, fatores de mercado, pessoais, sociais, culturais e psicológicos, pelo que é relevante reunir informação que permita entender como as pessoas interagem no meio social e como resulta a decisão de consumir (BASTA, MARCHESINI, OLIVEIRA e SÁ, 2006). Para a tecnologia atual, o *analytics* cumpre um papel fulcral neste sentido, em tempo real e com resultados satisfatórios.

Ainda no plano comercial, a fidelização dos clientes é baseada em descobrir o nível de satisfação dos mesmos, sendo dividida em:

- Identificação imediata dos problemas e
-Soluções.

Desta forma, os setores Bancário e Financeiro através da solução dos problemas que são apresentados, conseguem aprimorar e aperfeiçoar os serviços prestados com maior personalização dos seus produtos e serviços. O que resulta na mesma esfera de abordagem que engloba o conceito precedente, que inclui:

-Monitorização de comportamentos;
-Preferências e
-Analise de padrões de consumo.

Dado o exposto, pode-se chegar a conclusão de que o uso de *Big Data* é de suma importância e consegue abranger todos os setores que dependam de análises de dados pessoais, com o intuito de salvaguardar os interesses das pessoas.

O plano decisório está relacionado com a racionalidade na tomada de decisões, tanto pelo lado dos setores Bancário e Financeiro, como pelo lado dos clientes.

Do lado dos clientes, as tomadas de decisão são ser realizadas de forma consciente e seguem etapas que são determinadas pela teoria, iniciando por um problema (BAZERMAN e MOORE, 2010), a veracidade do problema apresentado (GOMES, 2007), e a verificação de alternativas (BAZERMAN e MOORE, 2010; GOMES, 2007; CHOO, 2016). Desta forma, observa-se a cautela com que o processo deve ser realizado, sendo a decisão direcionada para aplicações de valores, créditos, contratos bancários, entre outros.

Em relação ao lado dos setores Bancário e Financeiro a avaliação dos clientes é feita de forma mais rigorosa, que se divide em:

-Globalmente e

-Individualmente.

Globalmente está direcionado ao risco da carteira e individualmente ao potencial risco de cada cliente. A questão do risco não está somente direcionada com a precaução das empresas em auferir lucros ou não, sendo principalmente derivado de deveres legais. O risco de incumprimento nas relações é gerador de pontuação positiva ou negativa (no caso de materialização do risco) dos clientes. O recurso ao uso de *Big Data* facilita a identificação de perfil de risco, onde o crédito da pessoa será positivo ou negativo conforme o risco que cada pessoa possa apresentar.

O plano regulatório talvez seja o mais complexo dos referidos, ora porque a matéria é nova, ora porque a legislação deve acompanhar as rápidas mudanças no mercado, resultando num difícil acompanhamento para o cumprimento de exigência de regulação.

A tecnologia digital, ofertas de serviços *on line*, nova geração de pessoas exigentes e a confiança dos mesmos na tecnologia tem resultado na proliferação da *Fintech*[220], que oferecem serviços financeiros mais ágeis, com menos burocracia e custos reduzidos, como sistemas de pagamento, operações de crédito e gestão financeira, normalmente realizadas pelas *startups*[221](LEAL, 2017).

---

[220] São empresas de tecnologias que oferecem aumento da eficiência nas operações financeiras. É um novo modelo de negócio que favorece o aumento das oportunidades de escolha e formas de acesso aos serviços, com rapidez, convenientes, competitivas e custos reduzidos. As empresas que são associadas a estas novas tecnologias podem assumir um papel de maior importância como concorrentes dos serviços financeiros tradicionais, introduzindo e aumentando a concorrência num mercado concentrado, tradicional e pouco contestável. Autoridade da Concorrência em Portugal - Inovação Tecnológica e Concorrência no Setor Financeiro em Portugal. [Em linha]. [2018]. [Consult. 4 jan. 2019]. Disponível em WWW:<URL:http://www.concorrencia.pt/vPT/Noticias_Eventos/Comunicados/Documents/Vers%C3%A3o%20Final%20Issues%20Paper%20FinTech.pdf>.

[221] As *Startups* são uma forma de empresas voltadas para oferecer serviços que prezam pela agilidade e rapidez. São empreses que inicialmente possuem como característica a incerteza de sucesso, porém com ideias aparentemente rentáveis. As *startups* surgiram, de forma mais popular, no Vale do Silício (Silicon Valley), situado na Califórnia, como exemplo de sucesso as empresas que eram *startups* no início das suas atividades são: Google, Apple Inc., Facebook, Yahoo!, Microsoft, entre outras. Go2Web - Visualizando 15 anos de aquisições pela Apple, Google, Yahoo, Amazon e Facebook. [Em linha]. [2018]. [Consult. 23 jan. 2019]. Disponível em WWW:<URL:http://www.go2web.com.br/en-US/blog/visualizando-15-anos-de-aquisicoes-pela-apple-google-yahoo-amazon-e-facebook.html>.

A Comissão Europeia, observando o desenvolvimento do uso de *Big Data* nas vidas das pessoas, e em especial o grande desenvolvimento das empresas *Fintech*, tomou medidas[222] no sentido de regular as atividades no setor. A Comissão possui como objetivo tornar o mercado mais seguro nas transações financeiras e de acesso mais facilitado para os futuros operadores. Alega que a Europa possui potencial para se tornar "plataforma mundial para a *FinTech*", baseado nas vantagens que o mercado único oferece. Sendo as primeiras alterações regulamentares um apoio para melhorar o financiamento coletivo (*crowdfounding*), alega que o setor financeiro deva também beneficiar dos avanços tecnológicos tais como:

-Tecnologia de cadeia de blocos (*blockchain*[223]);

-Inteligência Artificial e

-A computação em nuvem (*cloud computing*).

Também no plano regulatório merecem destaque as empresas *RegTech*[224], que têm como objetivo oferecer soluções tecnológicas avançadas para as necessidades de conformidade legal dentro do setor financeiro. Também conhecida como *"nova FinTech"*, permite a distribuição automatizada de dados e relatórios normativos, por meio de análise de *Big Data*, sendo as atividades em tempo real e na nuvem.

A *RegTech* utiliza meios tecnológicos como:

- Computação em nuvem (*cloud computing*);

-*Big Data* e

- Tecnologia de cadeia de blocos (*blockchain*).

Na esfera *Big Data*, os objetivos são:

-Deteção de fraudes;

---

[222] Comunicado de imprensa da Comissão, que revela um Plano de Ação sobre a forma de tirar partido das oportunidades geradas na área dos serviços financeiros (*FinTech*) pela inovação tecnológica. Comissão Europeia - *FinTech*: Comissão adota medidas para um mercado financeiro mais competitivo e inovador. Em linha]. [2018]. [Consult. 24 jan. 2019]. Disponível em WWW:<URL:http://europa.eu/rapid/press-release_IP-18-1403_pt.pdf>.

[223] *Blockchain* pode ser traduzido em Português por cadeia de blocos. Tal tecnologia tem como objetivo permitir manter um registo público gerido de forma distribuída, sem intervenção de uma autoridade central. O facto de o registo ser distribuído por integrantes e gerido por eles, que são agentes independentes e autónomos, permite que a tecnologia possa ser útil quando não existe uma autoridade única como os bancos por exemplo, o que confere uma maior credibilidade ao sistema. ARAÚJO, Henrique Pereira de Araújo e ARAMBASIC, Rebecca Bignardi - A Tecnologia Digital Blockchain: Análise Evolutiva e Pragmática. [Em linha]. [2017]. [Consult. 17 jan. 2019]. Disponível em WWW:<URL:file:///C:/Users/vicen/Downloads/98-382-1-PB.pdf>.

[224] *RegTech* foi uma das tecnologias apresentadas durante a conferência de primavera de 2017 da TIC. Realizada em Luxemburgo em 11 de maio de 2017 e reuniu mais de 5000 participantes de cerca de 500 empresas e 70 países. UMULISA, Lise - *Deloitte and Digital zooms in on blockchain RegTech at ICT Spring*. [Em linha]. [2017]. [Consult. 22 dez. 2018]. Disponível em WWW:<URL:https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-pr-deloitte-digital-blockchain-regtech-ict-spring-11052017.pdf>.

-Operações ilegais;

-Identificação e categorização de clientes e

-Gestão de riscos das instituições financeiras, (CORDEIRO, OLIVIRA e DUARTE, 2017).

Por tudo isto, pode-se alegar que o mercado financeiro com as últimas inovações tecnológicas, possui a capacidade de potencializar o desenvolvimento do mercado. As soluções que a *FinTech* dispõe para automatizar a *compliance* levando ao *reporting* para a Autoridade de Supervisão de forma automática e em tempo real, contribui para melhorar a fiscalização das atividades financeiras.

6.6 Aplicação de Coimas

Pode-se alegar que a questão das coimas despertou a atenção de todos que trabalham com dados pessoais. A aplicação da mesma está prevista no Art.º 83.º combinado com o art.º 58.º, n.º 2, i) do RGPD, tendo a competência pertencer a Autoridade de Controlo de cada Estado-Membro.

Deverá ser analisada em cada caso individual, efetiva, proporcionada e dissuasiva. Nem sempre será de imposição imediata a aplicação de coimas quando existir violação ao RGPD, pode ser feita uma repreensão em vez de ser aplicada uma coima, dependendo das circunstâncias dos factos ocorridos. Deverá se ter em consideração a natureza, gravidade e duração da infração, se houve caráter doloso, quais as medidas tomadas para tentar atenuar os danos sofridos, também cabendo analisar o grau de responsabilidade ou eventuais infrações anteriores. [225] A coima máxima pode atingir 4% do volume de negócios anual ou €20 milhões.

CAPÍTULO VII – CONCLUSÕES

7.1 Conclusões

Diante do até agora exposto, pode-se afirmar que a velocidade, amplitude e profundidade com que as novas tecnologias se estão a desenvolver, através da interligação das mesmas com as pessoas, resulta numa mudança nas relações humanas e consequentemente na esfera jurídica das mesmas.

[225] Considerando 148 do RGPD

Como na maioria das situações nem tudo é eterno. Nem o Estado é eterno, precisando de se adaptar à evolução do tempo, como foi o caso da República Christiana da Idade Média, que ao adaptar-se às mudanças, transformou-se nos Estados complexos do mundo atual. Assim, o Estado moderno não é coisa permanente e eterna, sendo somente um momento no tempo histórico segundo Lasky (1939, p.5).

No âmbito desta dissertação, objetivou-se fazer sumariamente, uma abordagem das novas tecnologias que resultaram no fenómeno *Big Data*. E como não poderia ser diferente, analisar o RGPD e os impactos nas relações jurídicas que são estabelecidas, graças à velocidade da produção de informação.

Ocorre que, a tecnologia *Big data* apresenta-se atualmente como uma ferramenta a ser utilizada por diversos setores, sendo os titulares de dados pessoais o outro lado da relação, muitas vezes de uma relação *online*, pode-se, portanto, dizer que serão o lado mais frágil da relação, merecendo atenção especial.

Uma vez constatado que há tendências para que o arcaboiço jurídico fique rapidamente defasado frente à evolução da tecnologia, devido à rapidez desta, observa-se no entanto que o direito fundamental em questão já estava amparado pelo Art.º 8º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia e no Art.º 16.º, n.º 1 do Tratado sobre o Funcionamento da União Europeia, em que já era estabelecido que todas as pessoas têm direito à proteção dos dados de caráter pessoal.

O RGPG traz algumas novidades como a abordagem baseada no risco e a abordagem de autodefesa, que visam a melhoria da norma para se conseguir a proteção efetiva dos dados pessoais. No contexto de novas tecnologias, foi importante enfatizar os meios adequados que favorecem a defesa das pessoas, como exemplos: os princípios, os direitos, a abordagem baseada no risco e a abordagem de autodefesa, a avaliação de impacto e a consulta prévia à autoridade de controlo entre outros.

Não nos parece razoável fazer um comentário completo do RGPD, mas apenas abordar os meios no que toca ao tratamento de dados pessoais em larga escala, objetivando alcançar os meios adequados para a defesa dos mesmos e garantir um Estado de Direito Democrático para todos.

Pode-se dizer então que os hábitos das pessoas e a convivência em sociedade foram alterados pelo desenvolvimento atual da tecnologia, transformando-as numa fábrica de produção de dados. Esta produção inclui desde todos os dados que formam o seu perfil como pessoa, incluindo por exemplo informação de geolocalização, a dados sobre sua atividade académica e profissional (documentos), onde se desloca e o que vê (fotografias),

etc., tudo o que é possível de ser digitalizado, ou seja, tudo. Tal cria um verdadeiro fluxo de dados num caos entre dados estruturados, semiestruturados e não-estruturados.

A rápida evolução tecnológica a que se está a assistir, mostra-se desafiadora para os operadores do direito, deixando para traz os meios clássicos do direito à proteção de dados pessoais, e procurando estabelecer um direito novo, com base tecnológica, que deve ser desenvolvido concomitantemente à evolução tecnológica, nunca deixando de se valer do direito clássico nas matérias em que a lei especial não disponha soluções adequadas.

Pode-se concluir que, houve uma tentativa de adequação da legislação sobre dados pessoais em face ao desenvolvimento tecnológico, pois, a Diretiva que regulava a matéria já era de 24 de outubro de 1995. Seria inadmissível a matéria continuar a ser regulamentada por uma norma de 1995, face ao exposto da evolução tecnológica atual.

Prezando pela praticidade, estas são as características mais importantes do RGPD:

I) Reforço dos deveres de informação aos titulares dos dados;

II) Obrigatoriedade de informar a base legal para a realização da recolha, tratamento, conservação dos dados pessoais;

III) Fim do controlo prévio realizado pela CNPD, com a responsabilização direcionada às entidades públicas e privadas;

IV) Reforço dos direitos já existentes, incluindo o direito à limitação do tratamento e a portabilidade dos dados;

V) Inclusão de novos requisitos para a eliminação ou retificação de dados;

VI) Condições mais rigorosas do Consentimento para o tratamento dos dados pessoais;

VII) Novas exigências de tratamento de dados sensíveis e a inclusão dos dados biométricos;

VIII) EPD de nomeação obrigatória em certas situações;

IX) Obrigatoriedade do registo de atividades de tratamento de dados pessoais;

X) Obrigatoriedade do registo de atividades de tratamento de dados pessoais feito pelo subcontratante;

XI) Exigência de segurança no tratamento dos dados pessoais e de políticas de privacidade;

XII) Implementação de medidas como a avaliação de impacto sobre a proteção de dados e a Consulta prévia e

XIII) Implementação de coimas mais pesadas, nos casos de desconformidade com a legislação.

Mesmo assim, chega-se a conclusão de que o RGPD ainda não ampara com satisfação algumas matérias, como por exemplo os *Data brokers*, sendo os dados pessoais como produto de compra e venda ainda um problema atual e emergente; falta um conjunto de regras direcionadas ao tratamento de *Big Data*; falta regulação no sentido de saber se existe ou não coação quando se utiliza meios psicológicos para alcançar resultados financeiros; entre outros.

Foi possível verificar que o Regulamento Geral de Proteção de Dados inovou em alguns pontos, porém, manteve muita matéria já tutelada na Diretiva 95/46/CE, ora revogada.

A questão que se apresenta à luz do Regulamento Geral de Proteção de Dados é a seguinte:

- Até que ponto se admite a recolha de dados pessoais na internet, e em que momento pode essa informação ser usada na esfera dos negócios jurídicos?

Sendo o conteúdo *Big Data* o resultado do uso das novas tecnologias, principalmente as redes sociais, a *IoT*, o armazenamento em nuvem entre outras, os dados que são recolhidos e tratados e que constituem o *Big Data*, podem ou não ser dados pessoais. Nos casos dos dados pessoais, está a pisar-se num terreno de um direito complexo, muito debatido e estudado há muito tempo. Cabe destaque a autodeterminação informacional que possui ligação direta com o Consentimento.

O Consentimento é a resposta mais adequada que foi encontrada, mesmo na fase pré-contratual, pelo que o recurso aos meios tecnológicos deve ser feito de forma explícita e informada às pessoas. Nenhuma outra forma que possa ser apresentada como alternativa para justificar a recolha e o tratamento de dados pessoais no ciberespaço será lícita, se não for de acordo com os meios apresentados no RGPD, ou seja, o Consentimento como sendo um ato positivo, claro, de vontade livre, específica, informada e inequívoca conforme Art.º 4º, n.º 11 do RGPD. Não se pode deixar de observar que há outras formas de tratamento que estão reguladas no Art.º 6.º, n.º 1 da mesma norma. O RGPD é o instrumento que tem como finalidade harmonizar o amparo legal neste sentido, sendo uma das medidas que visam o mercado único europeu.

Sendo certo que a proteção de dados pessoais não pode e nem nunca vai favorecer a criação de formas de barreiras técnico-digitais na Europa, nem nos países que realizam atividades com a mesma, e dado que a sociedade da informação continuará no seu ritmo de desenvolvimento, cabe aos aplicadores do direito a investigação e a dedicação de tutelar os direitos das pessoas de forma harmoniosa e compatível com toda esta evolução digital.

7.2 Contributo da investigação

Esta dissertação é direcionada para os aplicadores do direito, procurando contribuir para o desenvolvimento da legislação e a tutela dos dados pessoais, em especial as relações baseadas por dados advindos através do *Big Data*.

Também procura contribuir para um melhor conhecimento da matéria apresentada por parte de quem se conecta na internet e que não quer ser tolhido de usar essa ferramenta tecnológica por receio de ter os seus dados pessoais violados ou usados de forma a prejudicar os seus interesses.

As organizações que tratam dados pessoais em massa devem sempre nortear o seu uso pela ética da informação no mundo dos dados. Esta ética de base tecnológica deve ser de uso universal, uma vez que na internet não existem barreiras. Sendo certo que o direito de base tecnológica deverá ser também universal.

O ambiente virtual aparentemente invisível ou imaterial, não pode ser tratado como se não existisse de facto. Existe e tem o poder de unir pessoas, dispositivos e estabelecer negócios com consequências jurídicas para todos.

Com a análise realizada sobre o RGPD, procurou-se também contribuir para questões ausentes ou pouco esclarecidas da norma. Quanto mais pessoas estudarem e questionarem sobre os direitos fundamentais que norteiam a matéria, maior é a possibilidade de terem os seus direitos devidamente protegidos.

7.3 Limitações da investigação

Baseado no RGPD e as inovações que a norma apresenta, não se objetivou analisar a legislação em toda a sua amplitude. A análise apresentada é apenas direcionada aos dados em larga escala e suas consequências, como a segurança dos dados pessoais dos utilizadores da internet.

7.4 Sugestões para investigação futura

A investigação e a sua importância para a vida dos aplicadores do direito que foi apresentada nessa dissertação, é o primeiro passo de todas as outras etapas que se seguirão. Existem melhorias e aprofundamentos possíveis de fazer nesta dissertação, um processo que necessitará de tempo mais alargado.

Em relação à questão dos efeitos na esfera da transparência do uso de *Big Data* como fator influenciador das pessoas no campo da coação, também será cabível o alargamento e aprofundamento do tema.

Quanto às tecnologias em si, em especial a *IoT* e a nuvem, que ganham grande importância no mundo *Big Data*, é apelativo o seu aprofundamento tendo em conta todo o contributo para a vida moderna.

Finalmente pode-se considerar um processo de dedicação aos estudos das novas tecnologias como fundamental, sendo o direito de base tecnológica imprescindível nos tempos atuais, devendo ser desenvolvido por todos os profissionais do direito.

Referências Bibliográficas

DOCUMENTOS IMPRESSOS

ATAÍDE, Rui Paulo Coutinho de Mascarenhas – Direito ao Esquecimento. **Revista de Direito Civil**. (2018), p. 4.

BONAVIDES, Paulo - **Curso de Direito Constitucional**. 18ª. Edição. São Paulo: Malheiros, 2006.

BORRUSO, Renato - ***Computer e Diritto II- Analisi giuridica del computer***. *Milano: Giuffrè*, 1989.

BAZERMAN, Max e MOORE dan. - **O Processo Decisório**. Rio de Janeiro: Elsevier, 2010.

BASTA, D., MARCHESINI, F. R.; OLIVEIRA, J. A., & SÁ, L. - **C. Fundamentos de Marketing**. 7ª Edição. Rio de Janeiro: Editora FGV, 2006.

CASTRO, Catarina Sarmento e - Os ficheiros de crédito e a proteção de dados Pessoais. **Revista de Estudos de Direito do Consumidor**. (2002). Centro de Direito do Consumo da Faculdade de Direito de Coimbra. 4 vol., n.º 4.

CASTRO, Catarina Sarmento e - **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005. ISBN 978-97-2402-424-0.

CANOTILHO, José Gomes e MOREIRA, Vital - **Constituição da República Portuguesa - Anotada** - Volume I - Artigos 1º a 107º. Coimbra: Coimbra Editora, 2014. ISBN: 9789723222869.

CLARO, João Martins - **O Princípio da Igualdade, in Nos Dez Anos da Constituição**, obra coletiva. Lisboa, 1987.

COMTE, Augusto – ***Politique Positive***. 1890, I, p. 351.

CORDEIRO, António Barreto Menezes - **Direito inglês dos contratos I - Formação, Conteúdos, Vícios**. Lisboa: AAFDL, 2017.

CORDEIRO, António Menezes - **Tratado de Direito civil II**. 4ª Editora. Coimbra: Almedina, 2014.

CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo de e DUARTE, Diogo Pereira - ***Fintech* – Desafios da Tecnologia Financeira**. Coimbra: Almedina, 2017.

CARVALHO, Jorge Moraes - **Manual de Direito do Consumo**. Coimbra: Almedina, 2018. ISBN 978-972-40-7340-8.

CHAVES, Rui Moreira - **Regime Jurídico da Publicidade**. Coimbra: Almedina, 2005.

CALVO, José Lopez - ***Comentário Al Regulamento Europeo de Proteción de Datos***, Madrid: Sepin, 2017.

CHOO, Chun Wei - **A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões**. 2ª Edição. São Paulo: Senac, 2006.

COSTA, Francisco Bruto da e BRAVO, Rogério – ***Spam e Mail-Bomb*** **subsídios para uma perspetiva penal**. Lisboa: Quid Juris, 2005. ISBN 972-724-239-1.

CUEVA, Pablo Lucas Murillo de la e MANÃS, José Luís Piñar - ***El derecho a la autodeterminación informativa, Madrid, Fundación Coloquio Jurídico Europeo***. Madrid: Fundación Coloquio Jurídico Europeo, 2009.

CUKIER, Kenneth e MAYER-SCHÖNBERGER, Viktor - ***Big Data: A Revolution That Will Transform How We Live, Work, and Think***. London: John Murray, 2013.

ESPÍNDOLA, Ruy Samuel - Conceito de princípios constitucionais. **Revista dos Tribunais**. 2ª Edição. São Paulo: Ed. Revista dos Tribunais, 2002.

FARIA, Maria Paula Ribeiro de – Artigo 35º (Utilização da Informática). *In* MIRANDA, Jorge; MEDEIROS, Rui, coord. - **Constituição Portuguesa Anotada** Tomo I. 2.ª ed., Coimbra: Wolters Kluwer Portugal, 2010. ISBN 978-972-32-1822-0.

FURTADO, José Afonso – **Uma cultura da Informação para o Universo Digital**. Lisboa: Fundação Francisco Manuel dos Santos, 2012.

GOMES, L.F.A.M. - **Teoria da Decisão**. São Paulo: Thomson Lob, 2007.

HILDEBRANDT, Mireille **– *Profiling and the Identity of the European Citizen***. Suíça: Springer Science, 2008.

KOTLER, Philip; ARMSTRONG, Gary - **Princípios de Marketing**. 12ª Edição. São Paulo: Pearson Prentice Hall, 2007.

LASKY, Harold – **O Direito no Estado**. Lisboa: Inquérito, 1939.

LEAL, Ana Alves. In CORDEIRO, António Menezes; OLIVEIRA Ana Perestrelo e DUARTE Diogo Pereira – ***FinTech*****- Desafios da Tecnologia Financeira**. Coimbra: Almedina, 2017.

LOVELACE, Ada - **Notas à tradução.** *In***: *MENABREA, L. F Sketch of the analytical engine invented by Charles Babbage***. Scientific Memoirs, 1843.

LORENZETTI, Ricardo Luís - Informática, *ciberlaw y e-commerce*. **Revista de Direito do Consumidor**. n. 36. São Paulo: Revista dos Tribunais, 2000.

LOPES, J.J. Almeida – **Tratados Europeus Explicados**. 2.ª Edição. Lisboa: Vislis, 2002. ISBN 972-52-0143-4.

LUCON, Paulo Henrique dos Santos - Garantia do tratamento partidário das partes- Garantias Constitucionais do Processo Civil. **Revista dos Tribunais** Vol. 1. N. º 1. São Paulo: Ed. RT, 1999.

MIRANDA, Jorge e MEDEIROS, Rui de - **Constituição Portuguesa Anotada Tomo I**. Coimbra: Editora Coimbra, 2005.

MIRANDA, Jorge - **Manual de Direito Constitucional Tomo II**. Coimbra: Coimbra Editora, 1996.

MARCOS, Isabel Davara Fernández de - ***Hacia la estandarización de la protección de datos personales: Propuesta sobre una «tercera vía o tertium genus» internacional***. Madrid: La Ley, 2011. ISBN 978-84-8126-827-0.

MENDES, João Castro - **Direito Comparado**. Lisboa: AAFDL,1983.

MONCADA, L. Cabral – **Filosofia do Direito e do Estado** – 2.ª Edição, Coimbra: editora Coimbra, 2014.

PINHEIRO, Alexandre Sousa; COELHO, Cristina Pimenta; DUARETE, Tatiana; GONÇALVES, Carlos Jorge e GONGALVES, Catarina Pina – **Comentários ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018.

PINHEIRO, Alexandre Sousa - ***Privacy*** **e proteção de dados pessoais: a construção do direito à identidade informacional**. Lisboa: AAFDL, 2015.

PORTANOVA, Rui - **Princípios do processo civil**. 3.ª Edição. Porto Alegre: Livraria do Advogado, 1999.

PUTNAM, Robert D. - ***Bowling Alone – The Collapse and Revival of American Community***. Nova Iorque: Simon e Schuster, 2000.

ROCHA, António Manuel da e CORDEIRO, Menezes - **Da Boa-Fé no Direito Civil**. Vol. 1. Coimbra: Almedina, 1984, p.530.

REICHENBACH, Hans - ***Erfahrung und Prognose***. Wiesbaden: Springer Vieweg, 1983.

STEELE, Brian; CHANDLER, Jonh; REDDY, Swarna - ***Algorithms for Data Science***. Suíça: Springer, 2016. ISBN-13: 978-3319457956.

SKYRMS, Bryan - **Escolha e acaso**. São Paulo: Cultrix, 1966.

VIEIRA, Carla Iva - **Guia Prático de Direito Comercial**. Coimbra: Almedina, 2016.

VALE. S. - Inteligência Artificial & Redes Sociais: notas sobre um *bot* que odiava humanos. **Revista Interdisciplinar UVA**. Rio de Janeiro: Áquila, 2016.

VARELA, João de Matos Antunes - **Das Obrigações em Geral**. Almedina: Coimbra, 2017. ISBN 978-972-40-1040-3.

VASCONCELOS, Pedro Pais de - **Proteção de Dados Pessoais e Direito à Privacidade-in Direito da Sociedade da Informação**. Coimbra: Coimbra Editora, 1999. ISBN:972-32-0916-0.

VICENTE, Dário Moura – **Problemática Internacional da Sociedade da Informação**. Coimbra: Almedina, 2005.

DOCUMENTOS ELETRÓNICOS

Autoridade da Concorrência em Portugal - Inovação Tecnológica e Concorrência no Setor Financeiro em Portugal. [Em linha]. [2018]. [Consult. 4 jan. 2019]. Disponível em WWW:<URL:http://www.concorrencia.pt/vPT/Noticias_Eventos/Comunicados/Documents/Vers%C3%A3o%20Final%20Issues%20Paper%20FinTech.pdf>.

AUGUSTO, João C. - *Intelligent Environments: a manifesto*. Vol. 3, n.º 12 [Em linha]. [2013]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://hcis-journal.springeropen.com/articles/10.1186/2192-1962-3-12>.

ARAÚJO, Henrique Pereira de e ARAMBASIC, Rebecca Bignardi - A Tecnologia Digital *Blockchain*: Análise Evolutiva e Pragmática. [Em linha]. [2017]. [Consult. 17 jan. 2019]. Disponível em WWW:<URL:file:///C:/Users/vicen/Downloads/98-382-1-PB.pdf>.

AXELSSON, A. S.; SCHROEDER, R. - *Making it Open and Keeping it Safe: e-Enabled Data-Sharing in Sweden.* [Em linha]. [2014]. [Consult. 19 jan. 2019]. Disponível em WWW:<URL:https://journals.sagepub.com/doi/10.1177/0001699309339799>.

AKOKA, J., Wattiau, I., & LAOUFI, *N - Research on Big Data- A systematic mapping study.* [Em linha]. [2017]. [Consult. 05 jan 2019]. Disponível em WWW:<URL:https://www.sciencedirect.com/science/article/abs/pii/S0920548917300211>.

AFFAIRS, *European Parliament - Committee on Legal. Draft Report: with recommendations to the Commission on Civil Law Rules on Robotics*. [Em linha]. [2016]. [Consult. 06 abr. 2018]. Disponível em WWW:<URL:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-582.443+01+DOC+PDF+V0//EN >.

BASTOS, Miguel Brito – Contratos de Dados Pessoais. I Jornadas de Proteção de Dados e Empresas. Faculdade de Direito da Universidade de Lisboa – CIDP. [Em linha]. [2018]. [Consult. 12 jan. 2018]. Disponível em WWW:<URL:https://youtu.be/EyjKf9IJSK8>.

BARBOSA, Mafalda Miranda - *Data controllers e data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil. [Em linha]. [2018]. [Consult. 22 jan. 2019]. Disponível em WWW:<URL:https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5aaacd451ae6cf02516c4b66/1521143111492/2018-10.pdf>.

Brown University. [Em linha]. [2018]. [Consult. 12 dez. 2018]. Disponível em WWW:<URL:https://www.brown.edu/about >.

BOTÃO ALVES, Maria Beatriz - Mensagem Publicitária da iEra nos Pequenos Ecrãs em Conexão com o Consumidor. [Em linha]. [2014]. [Consult. 18 jan. 2019]. Disponível em WWW:<URL:https://comum.rcaap.pt/bitstream/10400.26/7150/1/b%27bot%C3%A3o.alves_FINAL.pdf>.

Comissão Europeia - *FinTech*: Comissão adota medidas para um mercado financeiro mais competitivo e inovador. Em linha]. [2018]. [Consult. 24 jan. 2019]. Disponível em WWW:<URL:http://europa.eu/rapid/press-release_IP-18-1403_pt.pdf>.

CORDEIRO, António Barreto Menezes - O Consentimento do Titular dos Dados no RGPD. **Revista de Direito e Tecnologia** [Em linha]. [2018]. [Consult. 11 jan. 2019]. Disponível em WWW:<URL:https://blook.pt/publications/publication/e772e2d8f7b4/>.

CORDEIRO, António Barreto Menezes – O tratamento de dados pessoais fundado em interesses legítimos. **Revista de Direito e Tecnologia** [Em Linha]. Vol. 1 [2019]. [Consult. 15 mai de 2019]. Disponível em WWW:<URL:https://blook.pt/publications/publication/29c85b840a65/?fbclid=IwAR3oZ8IJPPnm2qAz__w20CAr1WhdkG4Tbv4jjSFNBTo8Bs4oL_wm7LUP0mA>.

CNCS- Centro Nacional de Cibersegurança Portugal - A Internet das Coisas (IoT – *Internet of Things*). [Em linha]. [2017]. [Consult. 29 ago. 2018]. Disponível em WWW:<URL:https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/>.

DEAN, Jeffrey and GHEMAWAT, Sanjay - *MapReduce: A Flexible Data Processing Tool*. [Em linha]. [2010]. [Consult. 19 jan. 2019]. Disponível em WWW:<URL:https://cacm.acm.org/magazines/2010/1/55744-mapreduce-a-flexible-data-processing-tool/fulltext?mobile=false>.

DEAN, Jeffrey. Biografia. [Em linha]. [2010]. [Consult. 31 out. 2018]. Disponível em WWW:<URL:https://ai.google/research/people/jeff>.

Dicionário Priberam – Definição de Encriptação. [Em linha]. [2017]. [Consult. 05 dez. 2018]. Disponível em WWW:<URL:https://dicionario.priberam.org/encripta%C3%A7%C3%A3>.

DIAS, Valéria - Automação rompe limites entre digital, físico e biológico. USP. [Em linha]. [2018]. [Consult. 4 jan. 2019]. Disponível em WWW:<URL:https://jornal.usp.br/tecnologia/4a-revolucao-industrial-rompe-limites-entre-digital-fisico-e-biologico/>.

DUARTE, Diogo Pereira - A Portabilidade dos dados. I Jornadas de Proteção de Dados e Empresas. Faculdade de Direito da Universidade de Lisboa – CIDP. [Em linha]. [2018]. [Consult. 12 jan. 2018]. Disponível em WWW:<URL:https://youtu.be/zoUTP8eeuco>.

Dicionário Priberam – Definição de *APP*. [Em linha]. [2018]. [Consult. 05 out. 2018]. Disponível em WWW:<URL:https://www.priberam.pt/dlpo/app >.

Dicionário Priberam – Definição de insights. [Em linha]. [2018]. [Consult. 8 ago. 2018]. Disponível em WWW:<URL:https://dicionario.priberam.org/insight>.

E-commerce News - Empresas do varejo estão de olho no mCommerce, o futuro do comércio eletrônico. [Em linha]. [2018]. [Consult. 1 jan. 2019]. Disponível em: <URL:https://ecommercenews.com.br/artigos/tendencias-artigos/empresas-do-varejo-estao-de-olho-no-mcommerce-o-futuro-do-comercio-eletronico/>.

European Commission – Cookies. [Em linha]. [2018]. [Consult. 25 nov. 2018]. Disponível em WWW:<URL:http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm>.

FLORIDI, L. Philos - *Big data and Their Epistemological Challenge. In: Philosophy and Technology*. [Em linha]. [2012]. [Consult. 8 jan. 2019]. Disponível em WWW:<URL:URLhttps://doi.org/10.1007/s13347-012-0093-4>.

Folha de São Paulo - Leitura de 'termos e condições' de serviços na internet exige 4,5 horas. [Em linha]. [2017]. [Consult. 9 jan. 2019]. Disponível em WWW:<URL:https://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-condicoes-de-servicos-na-internet-exige-45-horas.shtml>.

GONÇALVES, Maria Eduarda - *The EU data protection reform and the challenges of big data*: *remaining uncertainties and ways forward*. P.11 [Em linha]. [2017]. [Consult. 6 out. 2018]. Disponível em WWW:<URL:https://www.tandfonline.com/doi/abs/10.1080/13600834.2017.1295838>
.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Orientações sobre os encarregados da proteção de dados (EPD) (WP 243 rev.01). [Em linha]. [2016]. p. 10. [Consult. 5 dez. 2018]. Disponível em WWW:<URL: https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf >.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679 (WP251rev.01). [Em linha]. [2017]. [Consult. 2 nov. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp251rev01_pt.pdf>.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Parecer 4/2007 sobre o conceito de dados pessoais (WP136). [Em linha]. [2007]. p.6. [Consult. 2 jan. 2019]. Disponível em WWW:<URL:https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Parecer 05/2014 sobre técnicas de anonimização (0829/14/PT GT216). [Em linha]. [2014]. [Consult. 20 jan. 2019]. Disponível em WWW:<URL:https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831045040634.pdf>.

Grupo de Trabalho do Artigo 29.º para a Proteção dos 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 (WP 248 rev.01). [Em linha]. [2017]. [Consult. 21 jan. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf>.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (WP250 rev.01) [Em linha]. [2017]. [Consult. 23 nov. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf>.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679 (WP259 rev.01) [Em linha]. [2017]. [Consult. 18 dez. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf>.

Grupo de Trabalho do Artigo 29.º para a Proteção dos Dados - Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e subcontratante» (WP169) [Em linha]. [2010]. p.77. [Consult. 1 dez. 2018]. Disponível em WWW:<URL:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>.

Grupo de Trabalho do Artigo 29.º - Orientações Sobre o Direito à Portabilidade dos Dados (16/PT WP 242 rev.01). [Em linha]. [2017]. [Consult. 5 dez. 2018]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf>.

GALEON, Dom; HOUSER, Kristin - *An AI Completed 360,000 Hours of Finance Work in Just Seconds*. [Em linha]. [2017]. [Consult. 07 abr. 2018]. Disponível em WWW:<URL:https://futurism.com/an-ai-completed-360000-hours-of-finance-work-in-just-seconds/>.

GRELLER, W. - *Reflections on the knowledge society*. [Em linha]. [2012]. [Consult. 24 nov 2018]. Disponível em WWW:<URL:https://wgreller.wordpress.com/2010/11/03/big-data-isnt-big-knowledge-its-big-business/>.

GHEMAWAT, Sanjay - Biografia. [Em linha]. [2010]. [Consult. 30 out. 2018]. Disponível em WWW:<URL:https://ai.google/research/people/SanjayGhemawat>.

Go2Web - Visualizando 15 anos de aquisições pela Apple, Google, Yahoo, Amazon e Facebook. [Em linha]. [2018]. [Consult. 23 jan. 2019]. Disponível em WWW:<URL:http://www.go2web.com.br/en-US/blog/visualizando-15-anos-de-aquisicoes-pela-apple-google-yahoo-amazon-e-facebook.html>.

GUARDIAN, *The- Londoners give up eldest children in public Wi-Fi security horror show*. [Em linha]. [2014]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause>.

HARTZOG, W. e SELINGER, E.- *Big data in small hands.* [Em linha]. [2013]. [Consult. 16 jan. 2019]. Disponível em

WWW:<URL:https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-in-small-hands/>.

INA - Características do RGPD. [Em linha]. [2018]. [Consult. 18 jan. 2019]. Disponível em WWW:<URL:https://www.ina.pt/index.php/formacao-noticias/1856-formacao-ina-rgpd>.

InfoWester - O que é Bluetooth? - [Em linha]. [2018]. [Consult. 8 dez. 2018]. Disponível em WWW:<URL:https://www.infowester.com/bluetooth.php#definicao>.

IDC Worldwide - *Big Data and Big Money: The Role of Data in the Financial Sector*. [Em linha]. [2016]. [Consult. 19 fev. 2019]. Disponível em WWW:<URL:https://ieeexplore.ieee.org/abstract/document/7945155>.

KLOTZ, Ulrich - *The New Economy, in Frankfurter Allgemeine Zeitung, Overview of Enterprises in Pratice.* [Em linha]. [2000]. [Consult. 26 nov. 2018]. Disponível em WWW:<URL:http://www.idemployee.id.tue.nl/g.w.m.rauterberg/presentations/2000[e]-klotz.pdf>.

LANEY, Douglas - *Develop a Financial Risk Assessment for Data Using Infonomics*. [Em linha]. [2019]. [Consult. 15 jan.2019]. Disponível em WWW:<URL:https://www.gartner.com/analyst/40872/Douglas-Laney>.

LEAL, Ana Alves - *Big data* e proteção de dados pessoais – Desafios à luz do Regulamento Geral de Proteção de Dados. **Revista Vida Judiciária**. [Em linha]. [2018]. [Consult. 28 jan. 2019]. Disponível em WWW:<URL:http://www.cidp.pt/Archive/Docs/f826818695653.pdf>.

LEE, I. - *Big Data: Dimensions, evolution, impacts, and challenges*. [Em linha]. [2017]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://www.sciencedirect.com/science/article/pii/S0007681317300046>.

LIEBOWITZ, Stan J. - *File-Sharing: Creative Destruction or Just Plain Destruction?* [Em linha]. [2004]. [Consult. 16 out. 2018]. Disponível em WWW:<URL:http://som.dallas.edu/capri/destruction.pdf>.

MASSENO, Manuel David – Protegendo os Cidadãos – Consumidores em Tempos de *Big Data*. [Em linha]. [2017]. [Consult. 3 nov. 2018]. Disponível em WWW:<URL:https://www.academia.edu/31787984/Protegendo_os_cidad%C3%A3os-consumidores_em_tempos_de_Big_Data >.

MCAFEE, A., & BRYNJOLFSSON, *E* - *Big Data: The Management Revolution*. [Em linha]. [2012]. [Consult. 22 dez. 2018]. Disponível em

WWW:<URL:https://hbr.org/2012/10/big-data-the-management-revolution>.

MANYIKA, James - *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation*. [Em linha]. [2017]. [Consult. 3 mai. 2018]. Disponível em WWW:<URL:https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.ashx>.

MAROUS, J. - *Big Data: Big Opportunity in Banking... Or Big B.S.*? [Em linha]. [2012]. [Consult. 5 dez. 2018]. Disponível em WWW:<URL:https://thefinancialbrand.com/26363/big-data-analytics-retail-banking-jm/>.

NATH, Trevir - *How Big Data Has Changed Finance*. [Em linha]. [2018]. [Consult. 12 jan. 2019]. Disponível em WWW:<URL:https://www.investopedia.com/articles/active-trading/040915/how-big-data-has-changed-finance.asp>.

NEWELL, S., & MARABELLI, M. - *Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'*. [Em linha]. [2016]. [Consult. 10 nov. 2018]. Disponível em WWW:<URL:http://marcomarabelli.com/Newell-Marabelli-JSIS-2015.pdf>.

PAPIC, Marko e NOONAM, Sean - Social Media as a Tool for Protest [Em linha]. [2011], [Consult. 2 dez. 2018]. Disponível em WWW:<URL: https: <//worldview.stratfor.com/article/social-media-tool-protest>.

PEIXOTO, João Paulo – Vigilância Eletrónica: uma realidade desconhecida para a generalidade dos portugueses. [Em linha]. [2014]. [Consult. 20 jan. 2019]. Disponível em WWW:<URL:https://comum.rcaap.pt/bitstream/10400.26/9217/1/Vigilancia.Electronica..pdf>.

PWC - *Where Have You Been All My Life? How the Financial Services Industry Can Unlock the Value in Big Data*. [Em linha]. [2013]. [Consult. 27 ago. 2018]. Disponível em WWW:<URL:https://www.pwc.com/us/en/industries/financial-services/library/viewpoints/unlocking-big-data-value.html>.

QUELLE, Claudia - *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing*, p.2 [Em linha]. [2017]. [Consult. 6 out. 2018]. Disponível em WWW:<URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2695398>.

Revisão da Instrução Normativa – Participa. [Em linha]. [2014]. [Consult. 26 jul. 2018]. Disponível em WWW:<URL:http://www.participa.br/revisao-da-instrucao-normativa-no-4-de-2014/instrucao-normativa-n-4>.

SAMARAJIVA, R., e LOKANATHAN, S. Using Behavioral - *Using Behavioral Big Data for Public Purposes: Exploring Frontier Issues of an Emerging Policy Arena.* [Em linha]. [2016]. [Consult. 6 nov. 2018]. Disponível em WWW:<URL:http://lirneasia.net/wp-content/uploads/2013/09/NVF-LIRNEasia-report-v8-160201.pdf>.

SAS - Evolução do *machine learning*. [Em linha]. [2018]. [Consult. 16 jan. 2019]. Disponível em: <https://www.sas.com/pt_br/insights/analytics/machine-learning.html>.

Rank MyApp - M-commerce - O que é e qual o diferencial para os negócios? [Em linha]. [2018]. [Consult. 15 jan. 2019]. Disponível em WWW:<URL:https://www.rankmyapp.com/pt-br/mercado/m-commerce-o-que-e-e-qual-o-diferencial-para-os-negocios/>.

SHALEV, Shwartz S. e BEN, David. S. - *Understanding Machine Learning: From Theory to Algorithms*. [Em linha]. [2014]. [Consult. 8 nov. 2018]. Disponível em WWW:<URL:http://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning/>.

SILVA, Luís Gonçalves da – O RGPD e o Impacto Laboral. I Jornadas de Proteção de Dados e Empresas. Faculdade de Direito da Universidade de Lisboa – CIDP. [Em linha]. [2018]. [Consult. 12 jan. 2018]. Disponível em WWW:<URL:https://youtu.be/k9hZQ3Gr4u4>.

SOUZA, Ramon de - Batemos um papo com o robô advogado que já venceu 160 mil contestações. [Em linha]. [2016]. [Consult. 07 abr. 2018]. Disponível em WWW:<URL:https://www.tecmundo.com.br/inteligencia-artificial/106644-batemos-papo-robo-advogado-venceu-160-mil-contestacoes.htm>.

SCHWAB, Klaus - *The Fourth Industrial Revolution: what it means, how to respond.* [Em linha]. [2009]. [Consult. 04 jan 2019]. Disponível em: <URL:https://www.weforum.org/agenda/2015/10/the-fourth-industrial-revolution>.

SIMITIS, Spiros - Revendo Privacidade em uma Sociedade da Informação. [Em linha]. [1987]. [Consult. 16 out. 2018]. em WWW:<URL:https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3952&context=penn_law_review>.

Serviço Nacional de Saúde – PDS – Plataforma de Dados da Saúde. [Em linha]. [2018]. [Consult. 27 out. 2018]. Disponível em WWW:<URL:https://spms.min-saude.pt/2013/11/pds-plataforma-de-dados-da-saude/>.

SUPRIYADI, Daniar - *Personal and Non-Personal Data in the Context of Big Data*. [Em linha]. [2017]. [Consult. 19 jan. 2019]. Disponível em WWW:<URL:http://arno.uvt.nl/show.cgi?fid=142300>.

SWEENEY, Latanya - *Simple Demographics Often Identify People Uniquely*. [Em linha]. [2000]. [Consult. 27 set. 2018]. Disponível em WWW:<URL:https://dataprivacylab.org/projects/identifiability/paper1.pdf>.

SCHWABE, Jürgen - Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. [Em linha]. [2006]. [Consult. 21 nov. 2018]. Disponível em WWW:<URL:https://www.kas.de/c/document_library/get_file?uuid=c0b3d47d-beba-eb55-0b11-df6c530ddf52&groupId=252038>.

TRANT, Jennifer e WYMAN, Bruce - *Investigating social tagging and folksonomy in artmuseums with steve museum*. [Em linha]. [2006]. [Consult. 12 jan. 2019]. Disponível em WWW:<URL:http://www.ra.ethz.ch/cdstore/www2006/www.rawsugar.com/www2006/4.pdf >.

TRANT, J. - *Studying Social Tagging and Folksonomy: A Review and Framework*. [Em linha]. [2008]. [Consult. 28 dez .2018]. em WWW:<URL:https://journals.tdl.org/jodi/index.php/jodi/article/view/269/278>.

TechTarget - *internet of things (IoT).* [Em linha]. [2017]. [Consult. 10 jan. 2019]. Disponível em WWW:<URL:https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>.

TOMLINSON, Raymond - *Official Biography*: Raymond Tomlinson. [Em linha]. [2018]. [Consult. 20 nov. 2018]. Disponível em WWW:<URL:https://www.internethalloffame.org/official-biography-raymond-tomlinson>.

The University of Edinburgh - *Big Data - Global Strategic Business Report* - Leading Players Are IBM, SAP, Oracle, HPE, Palantir, Splunk, Accenture, Del' PR Newswire. [Em linha]. [2016]. [Consult. 29 set. 2018]. Disponível em WWW:<URL:ttps://www.ed.ac.uk/>.

USENIX Association OSDI '04 - *6th Symposium on Operating Systems Design and Implementation.* [Em linha]. [2004]. [Consult. 13 out. .2018]. Disponível em WWW:<URL:https://www.usenix.org/legacy/event/osdi04/tech/full_papers/dean/dean.pdf consultado em 06/09/2018>.

UMULISA, Lise - *Deloitte and Digital zooms in on blockchain RegTech at ICT Spring.* [Em linha]. [2017]. [Consult. 22 dez. 2018]. Disponível em WWW:<URL:https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-pr-deloitte-digital-blockchain-regtech-ict-spring-11052017.pdf>.

VALLE, Alberto - O que é EdgeRank do Facebook e qual sua importância. [Em linha]. [2018]. [Consult. 16 jan. 2019]. Disponível em WWW:<URL:https://www.academiadomarketing.com.br/o-que-e-edgerank/>.

Waste 4 Think Cascais - Pay-as-you-throw. [Em linha]. [2017]. [Consult. 3 nov. 2018]. Disponível em WWW:<URL: https://ambiente.cascais.pt/pt/projetos/waste-4-think-cascais>.

WACHTER, Sandra - *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. [Em linha]. [2017]. [Consult. 12 jan. 2019]. Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469>.

WANG, Pei; LIU, Kai e DOUGHERTY, Quinn - *Conceptions of Artificial Intelligence and Singularity*. [Em linha]. USA: 301010 *Informatoin*. [Consult. 22 ago. 2018]. Disponível em WWW:<URL: https://www.mdpi.com/2078-2489/9/4/79/htm>.

JURISPRUDÊNCIA

Acórdão do Supremo Tribunal de Justiça n.º 679/05.7TAEVR.E2. S1 de 16-10-2014.

Acórdão do Tribunal Constitucional n.º 288/98, in, 40.º vol. Sobre a Autodeterminação informacional.

Acórdão do processo n.º C-543/09 TJUE (*Deutsche Telekom AG v Bundesrepublik Deutschland.*

Acórdão do Tribunal Europeu dos Direitos do Homem (TEDH), petição n.º 33783/09 acórdão Godelli c. Itália de 25 de setembro de 2012.
Acórdão do Tribunal Europeu dos Direitos do Homem (TEDH), petição n.º 32881/04 acórdão K.H. Eslováquia de 28 de abril de 2009.
Acórdão do Tribunal Europeu dos Direitos do Homem (TEDH), petição n.º 10454/83 acórdão Gaskin c. Reino Unido de 7 de julho de 1989.
Acórdão do Tribunal Europeu dos Direitos do Homem (TEDH), petição n.º 42326/98 acórdão Odièvre c. França [GS] de 13 de fevereiro de 2003.

LEGISLAÇÃO

Assembleia da República - Tratado de Lisboa. [Em linha]. [2008]. [Consult. 30 dez. 2018]. Disponível em WWW:<URL:https://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf>.
Carta dos Direitos Fundamentais da União Europeia n.º 2012/C 326/02. [Em linha]. [2012]. [Consult. 28 nov. 2018]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>.
Código Civil português - Decreto-Lei nº 47 344, de 25 de novembro de 1966.
CNPD - Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados. [Em linha]. [2018]. [Consult. 03 abr. 2019]. Disponível em WWW:<URL:https://fiscalidade.pt/wpontent/uploads/2018/12/regulamento_1_2018.pdf>.
Instrução Normativa n.º 4 de 20 de dezembro de 2018.
LEI 67/98 - A Jurisprudência e o Regulamento 2016/679 (RGPD). [Em linha]. [2018]. [Consult. 28 jan. 2019]. Disponível em WWW:<URL:https://estudogeral.uc.pt/bitstream/10316/48094/1/Big%20data%20ehealth%20autodeterminacao%20informativa.pdf>.
Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.